The Institute of
Risk Management

Risk Trends 2025

THE INSTITUTE OF OPERATIONAL RISK
Part of the IRM Group

irm

Risk isn't just for risk managers

Risk managers have never been more in demand, upskill yourself and become a valued asset to your organisation with an IRM Qualification.

Find out more

1 A Word from our Chair

2 Risk Insights

5 Risk Trends Survey (CRO)

7 Infrastructure Group

12 Energy & Renewables Group

21 ESG Group

24 Charity Group

27 Cyber Group

36 Financial Services Group

39 Climate Change Group

46 IRM Ambassador Insights

49 IRM South East Asia Lead Insights

53 Australia Regional Group

56 East Africa Regional Group

60 India Regional Group

64 UAE Regional Group

68 North America and Caribbean Regional Group

72 South Africa Regional Group

A significant majority of global experts predict that the next decade will see the entrenchment of a multipolar or fragmented geopolitical landscape.

A word from our Chair

Stephen Sidebottom, IRM Chair

In an era of unprecedented change, understanding emerging risk trends is more crucial than ever. The IRM's Risk Trends publication goes beyond merely predicting outcomes, it focuses on the pace of change and the evolving challenges that businesses and boardrooms worldwide must face.

Reflecting on 2024, organisations grappled with a landscape marked by economic uncertainty, escalating geopolitical tensions, and rapid advancements in artificial intelligence. The past year underscored the volatility of global markets, the intensifying impact of climate-related events, and the growing complexity of regulatory demands. It was a year that reinforced the need for resilience, adaptability, and forward thinking risk management strategies more thann ever..

As we move through 2025 and beyond, organisations face a rapidly shifting landscape shaped by accelerating technological advancements, the global transition to renewable energy, geopolitical tensions, and tightening regulations on sustainability and governance. At the same time, longstanding risks, including climate change, cyber threats, economic instability, conflict, and public health vulnerabilities continue to evolve, demanding a proactive and strategic response.

The next decade is expected to be defined by a more fragmented geopolitical order, bringing both risks and opportunities to the forefront. In this environment, Enterprise Risk Management (ERM) is not just a safeguard it is a strategic enabler, equipping organisations to anticipate disruption, build resilience, and uncover competitive advantages. Risk professionals, particularly those with IRM qualifications, play a pivotal role in this transformation. Their expertise helps organisations move beyond risk mitigation to harness uncertainty as a driver of long term value.

With insights from IRM's global community, this year's Risk Trends report highlights how risk management is not only evolving as a discipline but also emerging as a cornerstone of business success in an increasingly complex world.

How is the world of risk changing?

Recognising that the nature of risk management has undergone a significant transformation in 2024, and will continue deep into 2025, will be key to risk practitioners worldwide as they develop their mitigation strategies.

The Institute of Risk Management itself is no exception to change, every passing year brings new challenges that must be addressed to grow and remain the leading body for Enterprise Risk Management (ERM).

Geopolitical instability has emerged as a dominant concern. Heightened tensions between major economies, shifting trade policies, and regional conflicts are introducing new layers of unpredictability for businesses and governments alike. The rise of economic nationalism, sanctions, and regulatory fragmentation is complicating global supply chains and increasing compliance risks.

Meanwhile, emerging economies are grappling with inflation, debt crises, and resource scarcity, adding further volatility to global markets. In addition, cyber warfare and state-sponsored attacks are escalating, forcing organisations to rethink their approach to digital resilience and national security risks.

What are the key shifts?

Driven by the explosion of technological advancements and increasing global uncertainties, we need to look at what the key shifts in risk are and how practitioners should prepare themselves, and their organisations, for the future. The ability to anticipate and respond to these fast moving developments will be crucial for risk practitioners in 2025.

These are:

1. Strategic Integration of Risk Management

2. Addressing Technology Driven Risks

3. Building Resilience in an Uncertain World

4. Emphasising ESG and Stakeholder Trust

5. Fostering Agile Risk Governance

What are the key shifts risk practitioners need to focus on in 2025?

1. Strategic Integration of Risk Management

Risk management is evolving from being a reactive function to becoming a strategic enabler. It is now essential to identify opportunities alongside risks and embed risk considerations into core business strategies. Scenario planning, predictive analytics, and stress testing are critical tools to help anticipate dynamic challenges and make informed decisions.

What practitioners should do:

- Build capabilities in strategic risk assessment, including scenario planning and risk forecasting.
- Foster closer collaboration with leadership to align risk strategies with business goals.
- Develop tools and dashboards that provide real-time insights into organisational risks and opportunities.

2. Addressing Technology Driven Risks

The proliferation of artificial intelligence (AI), automation, and digital transformation has introduced new risks, such as algorithmic bias, data privacy concerns, and cybersecurity threats. While these technologies enhance efficiency and innovation, they also demand a more nuanced approach to risk management.

What practitioners should do:

- Develop and implement robust cybersecurity frameworks, including zero-trust architecture and incident response plans.
- Collaborate with legal and compliance teams to address regulatory requirements related to AI, data protection, and privacy.

3. Building Resilience in an Uncertain World

The increasing frequency and complexity of global disruptions—such as geopolitical instability, supply chain challenges, and climate change—have made organisational resilience a top priority. A shift from short-term risk mitigation to long-term resilience planning is vital.

What practitioners should do:

- Conduct regular risk and resilience assessments, including supply chain mapping and geopolitical risk analysis.
- Diversify supply chains and establish contingency plans for critical dependencies.
- Develop crisis management plans and conduct regular simulation exercises to ensure preparedness.

4. Emphasising ESG and Stakeholder Trust

Environmental, social, and governance (ESG) risks are now central to organisational strategies. Climate change, regulatory pressures, and heightened stakeholder expectations are driving the need for stronger ESG risk management frameworks.

What practitioners should do:

- Integrate ESG considerations into ERM frameworks.
- Ensure compliance with evolving ESG reporting standards and regulations.
- Collaborate with sustainability teams to assess and mitigate climate risks, including transition risks.
- Engage stakeholders to maintain transparency and build trust through consistent ESG reporting and communication.

IRM Chair Insight - Agile Risk Governance

In a rapidly changing risk environment, agile governance is essential. This includes ensuring that risk management processes are flexible, dynamic, and integrated across all functions.

Preparing for 2025: Global Recommendations for Risk Practitioners

To stay ahead of the curve and prepare for the evolving landscape in 2025, risk practitioners around the world should:

Invest in Continuous Learning

- Pursue certifications in emerging areas such as AI ethics, ESG risk management, and cyber risk.
- Stay informed about global trends, regulatory changes, and technological advancements through industry groups, thought leadership, and professional networks.

Leverage Technology

- Adopt advanced risk management tools, such as AI-driven risk analytics, to enhance decision making.
- Use blockchain and other emerging technologies to ensure transparency and security in processes such as supply chain management.

Enhance Collaboration

- Build partnerships with external stakeholders, including regulators, industry peers, and technology providers, to share insights and develop industry standards.
- Collaborate across functions within the organisation to create a unified risk management approach.

Embed Sustainability into Risk Practices

- Integrate sustainability metrics into key performance indicators (KPIs) for risk management.
- Work with environmental and sustainability teams to address climate related risks and align strategies with global sustainability goals.

Focus on Risk Culture

- Promote a risk-aware culture by providing training and education to employees at all levels.
- Encourage transparency and communication around risks to foster a proactive mindset.

The future demands agility, collaboration, and a forward thinking mindset, ensuring that risk management continues to serve as a cornerstone of organisational resilience and success.

The future demands agility, collaboration, and a forward thinking mindset, ensuring that risk management continues to serve as a cornerstone of organisational resilience and success.

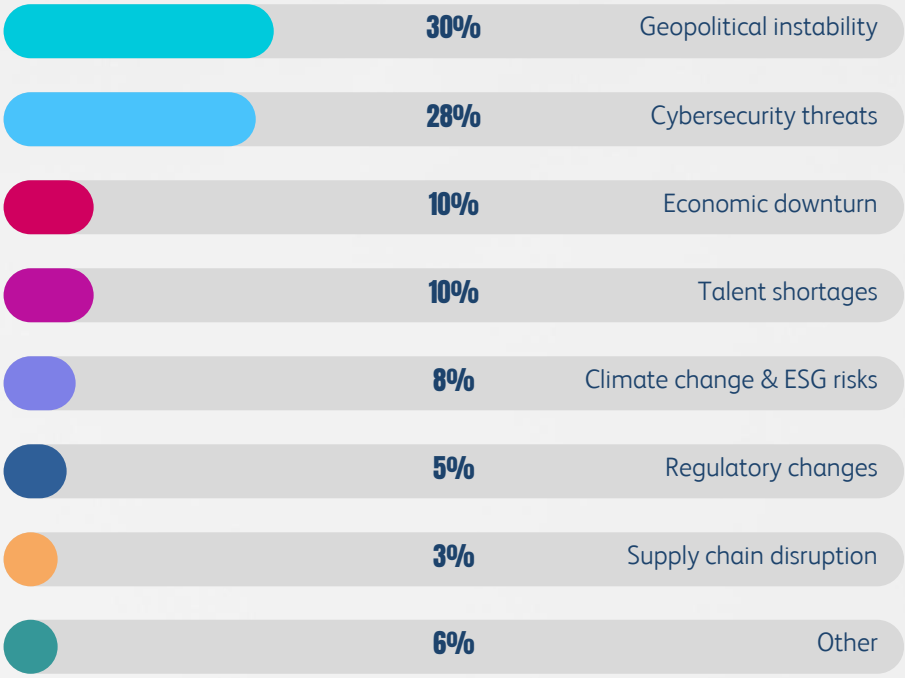
Risk Trends 2025 Survey

A global view of the future of risk

Interspersed throughout this report you'll find data and insights collected from over 250 risk practitioners from around the world.

In previous edition of IRM Risk Trends, we've focused on the opinions of our Special Interest and Regional Groups, and what their thoughts on the risk landscape will be in the coming year. This year, we also wanted to hear from you, our members and readers.

What do risk practitioners consider the top emerging risks facing organisations in 2025?



Which aspect of risk management has required the most significant investment or change in 2024?

- Practitioners highlighted Technology and Digital Risk Management as the most prominent concern, accounting for 37% of responses. Cybersecurity Infrastructure follows at 16%, emphasising the growing importance of digital security.
- Regulatory Compliance and Reporting and Employee Training and Awareness both received 11%, alongside Business Continuity Planning at 10%, indicating significant attention to operational resilience.
- Climate Risk Mitigation (8%) and Third-Party Risk Management (5%) were less prioritised, while other risk areas were mentioned by 2% of respondents.

CRO Insights

Picking the brains of those in charge

47% identified tech and digital risk as requiring the most investment and effort in 2024.

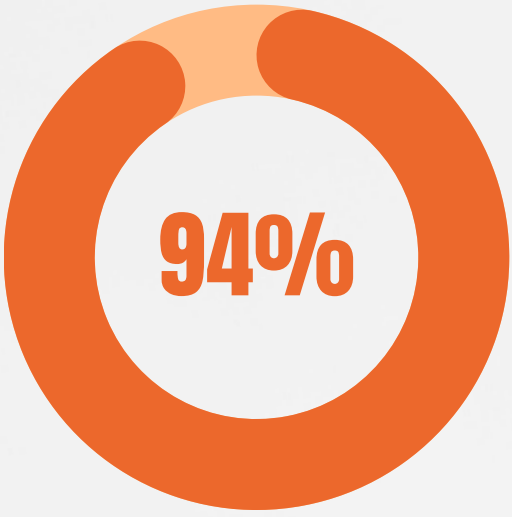
63% identified Cybersecurity threat and Geopolitical instability as the top emerging risks in 2025

86% indicated that it is difficult to recruit qualified risk professionals in their region.

44% indicated that the integration of risk management across different departments/functions was the biggest challenge in 2024.

42% believe they will become more strategic partners in business decisions in 2025

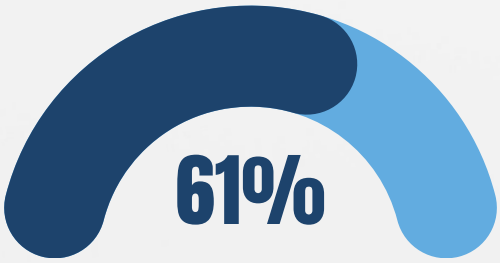
70% CROs believe that the demand for risk professionals is expected to increase in 2025 and beyond



94 % of Chief Risk Officers surveyed indicated that risk management as a career will evolve to require risk practitioners to develop and harness new skills in 2025 to meet the needs of new emerging risks.

63 % of these CROs expect that they will require advisory services within their organisations in 2025.

More and more CROs expect advisory services to be integrated into day to day decision making processes.



61 % CROs believe their industry will experience several regulatory changes in 2025.

01 Infrastructure Special Interest Group

Written by:
Yukitaka Matsuda
Chair, IRM Infrastructure Special Interest Group

Yukitaka Matsuda

Chair of the IRM Infrastructure Group and Senior Risk Manager at AtkinsRéalis. He has over 25 years of expertise in risk management, project management office, and business strategy across the manufacturing, infrastructure, and finance sectors. His qualifications include a Distinction in MSc Insurance and Risk Management, an MBA from LBS and Columbia Business School, an MSc in Engineering, NEC4 Project Manager Accreditation, and is an ACII and Chartered Insurance Risk Manager.

Written by:
Dr Robert Chapman
Risk Practitioner

Dr Robert Chapman

Robert has over 25 years' experience in the field of Risk Management across a wide range of industries including nuclear, rail, marine, road, telecommunications, IT, aviation, broadcast, health, sport, heritage, pharmaceutical, property, energy, utilities and more. He is a recognised expert in Risk Management and Optimism Bias, dedicated to enhancing business decision-making and project management. He has authored numerous books, papers, articles, and guidance documents on risk management, and provides specialised training in the field.

Written by:
Gareth Byatt
Risk Practitioner

Gareth Byatt

Gareth is an independent consultant specialising in urban resilience, disaster risk, and risk management and resilience across a wide range of industries and business sectors.

He is an Ambassador for the IRM. He regularly undertakes research work independently and with academic institutes around the world.

JOIN

The Infrastructure Group committee has identified potential risk trends for 2025, with a primary focus on the UK infrastructure sector. This report is based on recent UK Government announcements, international news, and reports from global organisations, and is structured into four sections: UK Infrastructure Demand Trends, the Contribution of Infrastructure to the UK Economy, Infrastructure Resilience and Sustainability Trends, and Global Trends (with a focus on the Middle East).

Infrastructure Demand in the UK

by Yukitaka Matsuda

Following the change in the UK Government this July, significant shifts are underway in the infrastructure sector. The Chancellor outlined a new growth strategy focused on three key pillars: stability, investment, and reform. Chancellor emphasised the urgency of taking immediate steps to build the infrastructure the UK requires. A key aspect of this approach includes reintroducing onshore wind projects into the Nationally Significant Infrastructure Projects regime, indicating that decisions on large developments will now be made at a national rather than local level. Additionally, the planning system is set for reform to ensure the delivery of critical infrastructure, and new policies are being developed to address infrastructure needs more effectively.

In September, the Chancellor also announced an Industrial Strategy aimed at driving long-term economic transformation. The strategy includes plans to establish Britain as a clean energy leader and accelerate progress towards net-zero emissions.

As part of this, ten new bills related to infrastructure have already been introduced, Planning and Infrastructure Bill, Passenger Railway Services (Public Ownership) Bill, Railways Bill, Better Buses Bill, High Speed Rail (Crewe to Manchester) Bill, Great British Energy Bill, English Devolution Bill, National Wealth Fund Bill, Water (Special Measures) Bill, and Budget Responsibility Bill. In October, the Chief Secretary to the Treasury reaffirmed the Government's mission of economic growth, citing a scenario where performance has matched the OECD average in monetary terms over the past 14 years. He reiterated the Government's commitment to delivering 'strategy and delivery' to fix the foundations of growth. These bills reflect the Government's shift toward a more proactive and integrated approach to infrastructure development. These bills could synergistically interact to enhance their collective impact, fostering new opportunities for UK infrastructure development and potentially driving growth unprecedented in recent decades, although they may introduce unforeseen risks.

> These changes in ecosystems may increase the demand for expertise in enterprise and project risk management for some projects, while decreasing it for others, as the project environment evolves.

For instance, the Better Buses Bill, which has already secured £955 million in funding to support bus services nationwide through 2026, is a prime example of this approach. Of this funding, £712 million is earmarked for local authorities to improve bus services, with £243 million allocated to bus operators.

Another example is the Railways Bill, which consolidates passenger services and network management under a single public body, Great British Railways. This restructuring of the rail sector will drive changes in the supply chain and ecosystem.

The Great British Energy Bill, which establishes Great British Energy, a government-owned clean energy company, will also reshape the ecosystem, aiming to reduce dependence on foreign energy supplies and minimise exposure to geopolitical risks. These changes in ecosystems may increase the demand for expertise in enterprise and project risk management for some projects, while decreasing it for others, as the project environment evolves.

The introduction of these new bills is also likely to impact the strategic objectives of some infrastructure projects, creating both threats and opportunities, particularly in terms of funding strategies. Furthermore, the Government's emphasis on attracting long-term investment may offer greater stability for project funding, potentially benefiting national projects in areas such as resource demand, project execution, sustainability, and quality.

Risk Managers should remain vigilant regarding potential impacts on cost, schedule, and scope, which could affect the successful project delivery.

Contribution of critical national infrastructure to the UK economy

by Dr Robert Chapman

Successive governments have recognised the part that our Critical National infrastructure (CNI) plays in the UK's economy. The UK government's National Infrastructure Strategy issued in 2020 sought to boost growth and productivity across the whole of the UK, level up investment and strengthen the Union.

It stated "infrastructure underpins the economy. Transport, digital, energy and utility networks are vital for jobs, businesses and economic growth".

In October this year, in his speech at Skanska's national HQ, Chief Secretary to the Treasury, Darren Jones, stated infrastructure is the very lifeblood of the country's economy, and that through it, working people are better connected with the opportunities they need, businesses can find the top talent they need, and Britain is better linked to the rest of the world.

During his speech, the Chief Secretary announced the creation of the new National Infrastructure and Service Transformation Authority (NISTA) with the goal of bringing infrastructure strategy and delivery together to address existing systemic delivery challenges. A catalyst for the initiative no doubt is that infrastructure development has not been without its issues.

In the strategy referred here, it states infrastructure had been held back by "stop-start public investment, insufficient funding for regions outside of London, slow adoption of new technology, policy uncertainty that undermines private investment, and project delivery plagued by delays and cost overruns".

There is a clear consensus that the UK's CNI plays a vital role in the UK's economy by ensuring the smooth functioning of essential services and supporting economic growth.

Here are some key contributions:

1. Economic Stability: The CNI sectors, such as water, energy, transport, and finance, are crucial for maintaining economic stability. They provide the backbone for our lives and businesses.

2. Investment and Growth: Significant investments are made in infrastructure projects, which drive economic growth. The current government recognises substantial investment in infrastructure is required, (jointly by the government and private enterprise), to support economic recovery and long-term growth.

3. Job Creation: Infrastructure projects create numerous job opportunities across various sectors, including construction, engineering, digital technology and space. This not only boosts employment but also enhances skill development and innovation for long term prosperity.

4. Regional Development: Investments in infrastructure help in regional development by improving connectivity, reducing disparities, and supporting local economies. Projects like the £36 billion Network North aimed to unlock significant transport benefits for towns, cities, and rural areas.

5. Resilience and Security: The CNI ensures the resilience and security of essential services, which is critical for national security, public safety and the economy. Protecting these infrastructures from cyber threats and other risks is a priority for the government.

Infrastructure Resilience and Sustainability Trends

Gareth Byatt

The need for infrastructure to be inclusively designed, constructed and maintained in a way that supports resilience for communities, nations and the world is paramount. As Kamal Kishore, Special Representative of the United Nations Secretary-General for Disaster Risk Reduction, and Head of the United Nations Office for Disaster Risk Reduction says in introducing the Global Assessment Report (GAR) Special Report 2024:

"As much of the infrastructure needed to support our growing human population has yet to be built, we owe it to future generations to leverage every opportunity to inject resilience into our investments. This starts with understanding the past to build a more resilient future."

Infrastructure needs to be appropriately designed to support disaster resilience. This requires meaningful engagement of all stakeholders, not assuming that "physical solutions" will always be the sole solution. Infrastructure around the world is advancing at pace.

Energy infrastructure is showing that clean energy can be affordable, and we believe this trend will continue. Transport & mobility infrastructure will hopefully continue a trend of investments in resilient public transport, whilst helping to tackle climate emissions, both in "embodied carbon" (emissions during construction) and "operational carbon" (emissions during operation). Telecoms infrastructure is improving and liberating lives.

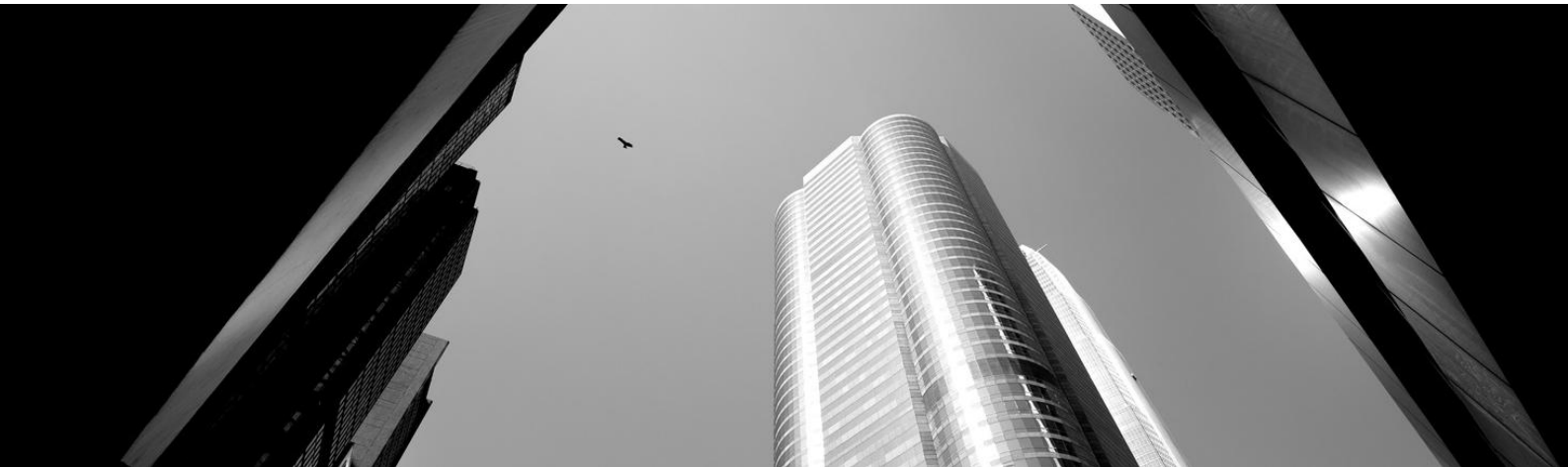
Infrastructure Global Trend

As the World Bank state: across much of the developing world, infrastructure remains woefully inadequate. One billion people live more than two kilometres from an all-season road; 675 million lack access to electricity at home; and nearly 4 billion people live without access to the Internet. We earnestly hope that this situation will improve during 2025. According to the World Bank's economic update in October 2024, the context for the Middle East is characterised by average modest GDP growth of 2.2% in 2024.

Whilst the wider region continues to focus on diversifying away from the oil sector, the main constraining factor on economic conditions continues to be focused on the combination of extended oil output cuts and downward pressure on oil prices. Despite the near-term economic challenges, there continues to be a continuing expansion of major infrastructure giga-projects across the region, including:

- NEOM, the 26,500km^2 development in the north of Saudi Arabia.
- Qiddiya, the 376km^2 entertainment landmark in Riyadh, the capital city of Saudi Arabia.
- The further development of Dubai's Expo 2020 site into District 2020, the country's first 15-minute city, a cycle-friendly, traffic-free suburb.
- Jeddah Tower, which will be the world's tallest tower, again in Saudi Arabia.

According to MEED, Saudi Arabia alone has a portfolio of 20 giga-projects with a total value of $850bn. Whilst the sheer scale and aggressive timelines of these projects will have a disproportionate effect on the global supply of key commodities (for example, at peak NEOM is estimated to require up to 20% of the world's steel supply), Arab News recently reported that, as a part of a wider review of its portfolio of infrastructure projects, Saudi Arabia may recalibrate its spending over the next several years.



02 Energy & Renewables Special Interest Group

Written by:
Grant Griffiths
Chair, Energy & Renewables Group

Grant Griffiths

Grant is an IRM Global Ambassador and chairs the IRM's Energy & Renewables Group. He has worked in the energy and related sectors in a 30+ year career working across the full spectrum of industry from developing liberalised energy markets, to working on ESG and the energy transition. He works with organisations in developing their enterprise risk & resilience, ESG and corporate governance capabilities for clients across UK, EMEA and South-east Asia. He is also an approved IRM trainer and a Senior Consultant with IRM Advisory.

Written by:
Dylan Campbell
Risk Practitioner

Dylan Campbell

Dylan is an internationally experienced award-winning risk management leader with over 20 years of risk management experience as an enterprise risk & resilience, business continuity and process safety leader, and project risk management specialist. Alongside his executive director position, he has extensive experience working with executive teams and boards and a passion and proven track record for building successful risk cultures within organisations. His recent publications include the ground breaking "Bitcoin and the Energy Transition: From Risk to Opportunity" published by the IRM which received global recognition.

Additional Contributors

- Myriam Bou Younes (Secretary)
- Alexander Larsen (Immediate Past Chair)
- Sean Gotora
- Beth Procter
- Dr Mykhailo Rushkovskyi
- Craig Bolley
- Dr Robert Chanon
- Afroze Miah

JOIN

Risk Trends for 2025

2024 has been another year characterised by geopolitical uncertainty and associated energy market speculation.

We've witnessed continuing volatility in markets, ongoing geopolitical events and shifts in traditional alliances, the continuing evolution and advancement of new technology developments and to top it off, significant changes to policy in key markets and the ushering in of a significant shift in US policy to come in 2025. We have already seen changes in the UK from the renewed impetus on moving towards net zero targets, changes to electricity market operations and the extension to operating dates for some of the UK's established nuclear power plants.

Following the 2024 US Presidential Election we anticipate further and significant changes to energy and related policies which will have implications far beyond domestic boundaries. We are already witnessing a period of relative calm for oil prices, despite the continuing uncertain environment and potential scenarios in the Middle East along with the expectation of OPEC+ adjustments yet to be felt in 2025.

With ongoing energy transition initiatives moving forward at pace, we envisage significant transitional, technical and financial risks to remain the order of the day.

Looking to global trade and supply chains, we can expect further complexities to interplay with both energy prices and investment. The contagion effect from geopolitical events in both Ukraine / Russia and China / Taiwan, to name just two, could have far reaching consequences, with a change to the status quo anticipated given the new White House administration taking office in January 2025.

While our predictions in these areas are in line with most industry commentators, we highlight the specific challenges in addressing the risks the industry will face across the entire value chain in terms of both their magnitude and their influence on longer-term strategic decisions.

Our outlook for the year ahead considers a wide range of factors, reflecting the complexity and wide range of opportunities in the world of energy as we look to create a sustainable, reliable and better future for the world and the energy industry.

As energy businesses, regulators and governments continue to drive forward with their agendas, the role of the risk manager will continue to gain importance, bringing insights to the increasing complexity and uncertainty these diverse stakeholders face. And there is still much more to be done.

The development and the role of the risk management profession in the energy sector continues to develop, adapt and grow, and we believe 2025 will be a year of significant advancement for the profession.

On a final note it is worth paying tribute to the ongoing work of our Group, and notably the dedicated efforts of our Committee.

At the end of 2023 we compiled our forward-looking views for the year 2024. Throughout the year we continuously reviewed and tracked the sector, markets, key risks and events, and our forecasts.

Now as we look back at the events that unfolded throughout the year – and the risks the energy sector faced – we are pleased to report that many of the trends we identified and flagged to the world materialised. That said, this does not mean the work of risk managers and the risk management profession are done – nor is our work as thought leaders in energy and risk. Far from it.

In this report we build on our work in 2024, looking at the key trends in energy for the year ahead. A complex array of factors that include evolving market dynamics, shifts in the regulatory environment, technological advancements, and geopolitical factors will weigh heavily on the sector.

We focus our observations on 6 key areas as follows:

- Geopolitical Instability
- Energy Transition
- High Performance Computing and Energy Grids
- Economic Instability's Role in Supply Chain Shocks
- Concentration & Monopolisation of AI in Energy Systems
- Off-shore Wind Sector

Here are the 6 risk trends we anticipate for 2025

1. Geopolitical Instability

Ongoing conflicts and political tensions, particularly in key oil-producing regions, pose risks to supply chains and market stability. While the Middle East remains a focal point for potential disruptions, events further afield also pose significant downside risks for reasons far beyond that of supply and demand.

The traditional nature of energy markets due to their economic importance means they are inherently sensitive to external events and factors. While geopolitical factors (not to mention other factors such as natural disasters) all pose significant risks to fossil-based fuels and their markets, the realities of the energy transition and the rapid technological advancements taking place, naturally means significant change to and a re-balance of energy sector value chains, which introduce new risks.

Concentrated supply chains and geopolitical tensions increase costs and cause project delays; dependencies on critical minerals and uneven technological readiness bring new considerations when it comes to geopolitical tensions which threaten the success of the energy transition.

Risk managers will need to undertake and heavily rely on more rigorous analysis of emerging risks, coupled with the use of scenarios that accesses high quality data and insights from a wider range of sources than may have been considered before.

The big things to keep an eye on include:

- China's Dominance: Controlling over 70% of global rare earth processing and 60% of lithium-ion battery production, China holds a strategic position, making other nations dependent.
- Resource Nationalism: Countries like Indonesia and the Democratic Republic of Congo have imposed export restrictions, prioritising domestic industries but straining global supply chains (the Democratic Republic of Congo supplies 70% of the world's cobalt, while Indonesia is a major source of nickel).
- New conflicts: New areas of conflict may emerge, caused by the fight for critical minerals which could be encouraged by ongoing uncertainty and instability.

2. Energy Transition

The global pivot from fossil fuels to renewable energy is reshaping industries and economies. The energy transition relies heavily on critical minerals like lithium, cobalt, and nickel, with supply chains dominated by a few nations, as well as technological innovation and large-scale investment supported by a homogenous, stable regulatory environment and markets being in a position to provide much needed funding for key energy transition projects.

As reflected in our first trend (Geopolitical Instability, above) the energy transition is highly exposed to risks from an escalating geopolitical landscape.

The global shift toward renewable energy is crucial for combating climate change. Uneven technological readiness, challenges from divergent regulations driven by national or regional policy agendas, and geopolitical tensions all threaten the success of the energy transition and risk delaying progress. Countries such as Russia are resisting the transition, forming alliances and maintaining fossil fuel production which remains the bedrock of their economy despite Western sanctions.

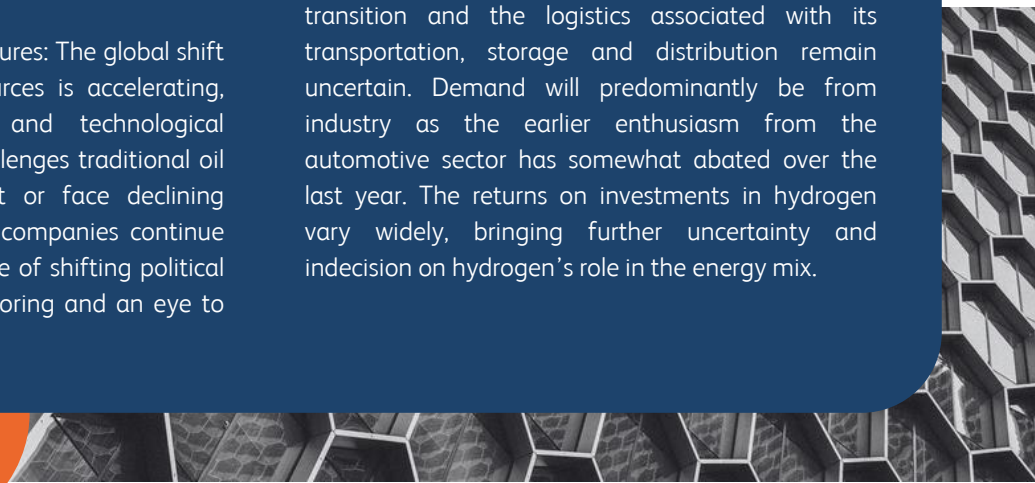
Competing blocs, such as the U.S.-led Minerals Security Partnership and China's Belt and Road Initiative, further fracture global energy governance; these in turn lead to a fragmentation which inflates the costs of renewable energy technologies (for example, inflationary factors include supply chain disruptions, abundance of cheaper fossil fuel alternatives, lack of readily available funding for transition initiatives) and exacerbate delays in energy transition for developing nations.

At a national level, the planned investments in boosting electricity grids in preparation for achieving transitional targets face challenges on several fronts: from government approvals and local authority planning processes, to timely availability of key components and services, and competition for talent to help design, build and maintain the infrastructure.

System operators and grid owners also face technical and operational constraints inherent with the current mix of thermal generators, oversupply of renewable energy, and their obligations associated with achieving security of supply.

The big things to keep an eye on include:

- Fossil Fuel Countermeasures: Oil-reliant nations such as Russia resist the renewable push, maintaining a key role in influencing fossil fuel supply and contributing to the fracturing of global energy governance.
- Photovoltaic (PV) Technology: China's dominance in PV manufacturing poses risks related to supply chain disruptions and geopolitical stability.
- Thorium reactors and SMRs: These present a transformative opportunity to revolutionise nuclear energy with safer, efficient, and environmentally friendly alternatives to conventional systems and technologies.
- Energy Transition Industry Pressures: The global shift towards renewable energy sources is accelerating, driven by climate policies and technological innovations. This transition challenges traditional oil and gas companies to adapt or face declining market relevance; how energy companies continue to respond especially in the face of shifting political imperatives require close monitoring and an eye to the longer-term future.
- Energy Transition Pressures from Investors: The real challenge is in satisfying the divergent and competing demands of a diverse stakeholder base. We anticipate more active intervention from investors in both renewables and traditional hydrocarbons businesses as they pursue acceptable levels of financial returns. This carries the risk of adversely impacting key actors in the complex renewables supply chain. And given the negative power prices experienced in 2024 due to an oversupply of renewable energy (which is difficult to curtail), the road ahead may present more risks than originally anticipated.
- Hydrogen: The role of hydrogen in the energy transition and the logistics associated with its transportation, storage and distribution remain uncertain. Demand will predominantly be from industry as the earlier enthusiasm from the automotive sector has somewhat abated over the last year. The returns on investments in hydrogen vary widely, bringing further uncertainty and indecision on hydrogen's role in the energy mix.



3. High Performance Computing and Energy Grids:

High Performance Computing (HPC), driven by the growth of AI data centres and Bitcoin mining operations, present both risks and opportunities to energy grids across the world and will require careful management to ensure the most efficient use and distribution of energy. The growth of artificial intelligence (AI) has transformed energy generation, distribution, and consumption, offering efficiency and resilience, but also creating threats to these systems. Similarly, we previously reported on the potential risks and opportunities associated with Bitcoin mining on energy grids.

Both AI data centres and Bitcoin mining operations fall under the umbrella of High Performance Computing and are energy-intensive, potentially creating challenges to distribution and load balancing. HPC applications like demand forecasting, renewable energy integration, predictive maintenance, and automated decision-making optimise grid performance while simultaneously delivering cost advantages and performance benefits to asset managers and owners. Yet these interconnected systems are vulnerable to systemic risks. Cybersecurity breaches, such as state-sponsored attacks, could exploit vulnerabilities, cascading failures across interconnected grids. Algorithmic errors, stemming from untested AI models or faulty data, may mismanage energy flow, causing widespread outages. Additionally, centralised HPC platforms heighten risks as single points of failure, while natural disasters could disrupt physical grid infrastructure and communication networks. The potential impacts of such a failure are severe. Data centre overloads have the potential to impair grid performance with significant performance and investment considerations.

Widespread blackouts would halt hospitals, transport, and communication systems, crippling global markets and industries reliant on stable electricity. Prolonged outages could trigger public unrest and political instability, especially in vulnerable regions. Although considered to be rare, a global HPC-driven energy grid failure would have profound consequences, making proactive measures critical. Balancing efficiency with resilience is key to safeguarding an HPC-powered energy future.

Mitigation strategies include decentralising distribution of HPC data centres, developing redundant systems for emergencies, and enhancing AI transparency and testing. Cybersecurity investments, such as zero-trust architectures, and international cooperation on AI ethics and grid management are essential to resilience. Grid operators, regulatory authorities, power producers and HPC business will all need to work together to ensure security of supply, grid resilience, limitation of energy waste and price stability. Bitcoin mining facilities also present opportunities to implement a hybrid HPC strategy as they are highly suited for hosting AI operations. With experienced personnel and a background in a competitive industry marked by Bitcoin's mining difficulty and halvings, these facilities are well-equipped for such a transition. It's not surprising that many are already shifting from exclusive Bitcoin mining to hybrid data centre operations. For instance, last October a bitcoin mining company, Australian Iris Energy (Nasdaq: IREN), partnered with WEKA to offer both storage and GPU stacks for generative AI.

The big things to keep an eye on include:

- Emerging economies: These economies struggle with integrating stranded renewable projects into outdated, poorly developed grids, leading to outages. Being location agnostic, HPC data centres will continue to offer opportunities to leverage stranded renewable projects in emerging economies, making the profitable, leading to further investment in energy infrastructure in those areas.
- Vertical Integration: As HPC operations and energy markets continue to converge and grow we will continue to see the energy infrastructure owners, bitcoin miners and AI data centre operators vertically integrate.
- Nation state investment: Recognising the strategic importance of HPC infrastructure, we will continue to see a growing trend of favourable regulatory policy and even direct investment in HPC projects by state actors as we have already seen in countries such as El Salvador, Bhutan, the Oman.

4. Economic Instability's Role in Supply Chain Shocks:

Global economic fragility, fueled by high sovereign debt, inflationary pressures, investor pursuit of returns, and ongoing trade wars, is creating a precarious environment for supply chains. A number of industries essential to the ongoing energy transition such as PV manufacturing - with over 80% of solar panel manufacturing concentrated in China – and others involved in the provision of resources and services - such as wind turbine and blade manufacturers - are particularly vulnerable.

Geopolitical tensions (as we have extensively discussed earlier) and ESG mandates are exacerbating the risk of supply chain bottlenecks.

Disruptions in the supply chain for critical components like polysilicon or lithium could derail renewable energy projects, slow down global energy transitions, and drive up costs, further exacerbating inflation.

There is a particular danger for developing economies that rely on affordable renewable energy technologies to meet their climate commitments.

A key strategy in tackling this challenge is to regionalise supply chains, explore ways of increasing transparency through the use of distributed ledger technologies, and investment in diversified procurement strategies.

The big things to keep an eye on include:

- Consideration of enhanced technologies: Aspects such as AI-driven supply chain optimisation, distributed manufacturing systems, and blockchain-based tracking for ESG compliance will also be factors which might come into play in the quest to overcome challenges and risks.

- Changes to investor strategies: This will depend on the global economic picture and the direction monetary policy (interest rates) take over the next 12 months. The extent to which government incentives are made available will also carry weight with investors.

- Government policy change: In order to realise their short to medium-term strategies, we are likely to see significant shifts in policy in some major economies.

Those committed to the realisation of energy transition targets will adjust their spending and investment focus to support renewables industries while those pursuing an economic growth agenda are more likely to address the bread and butter issues of reducing domestic inflation, taxation and incentives for value-added industries, irrespective of their sector.

- Climate Risks: Fragmented governance jeopardises international climate goals.

5. Concentration & Monopolisation of AI in Energy Systems:

Continuing on from the earlier theme of energy grids and HPC, the adoption of artificial intelligence (AI) in energy systems is transforming the energy value chain: grid management, renewable energy forecasting, demand side patterns, product development and storage optimisation, can all benefit from the unmatched efficiency and resilience AI offers. However, the growing dominance of a few major tech players poses significant risks to energy security, market competition, and innovation. If unchecked, monopolisation in this domain could lead to systemic issues, threatening global energy stability.

In our view, this is a looming Grey Rhino Risk.

The concentration of power among a few companies creates disproportionate influence over energy markets, risking anti-competitive practices such as price manipulation and preferential access to resources. For example, Tesla's dominance in energy storage and Google DeepMind's partnerships for grid optimisation centralise control over critical energy infrastructure. These systems also face heightened risks of cyberattacks; a breach in a dominant AI provider could cascade across multiple grids, causing widespread blackouts.

Market monopolisation stifles innovation by discouraging smaller companies from entering the field, limiting diverse and localised solutions, particularly in emerging markets. Additionally, proprietary systems lock utilities into long-term dependencies, making transitions to alternative providers costly and impractical.

Data privacy and sovereignty issues further complicate the landscape, as centralised platforms often cross borders, raising security concerns. Addressing these challenges requires fostering open-source platforms to reduce reliance on proprietary systems and encouraging regionalised AI development to diversify control. Governments should implement robust regulatory oversight and antitrust measures to prevent monopolistic practices.

Collaboration between public and private stakeholders is essential to broaden innovation and competition. Stringent cybersecurity protocols must also be mandated to minimise systemic risks. The European Union's AI Act, the world's first comprehensive AI law designed to provide some protections from the inherent vulnerabilities and risks in pursuing AI.

This measure specifically requires the uses of AI system or systems to be classified according to the risk they pose to users, with the intention being that those systems with higher risks require higher levels of oversight and regulation; for example, high risk systems used in the management and operation of critical infrastructure need to be registered in an EU database. While this is a step in the right direction, towards mitigating risks associated with the use of AI, it still requires organisations to fully assess and understand the risks and it, by no means, eliminates AI risks posed by the factors we have highlighted above, especially that of monopolisation and market dominance, and organisations need to remain vigilant to the risks posed by AI.

The big things to keep an eye on include:

- Regulation: Too often we have seen systemic failures take place, acting as the catalyst for reactive government action and intervention. How and if governments will move to implement effective strategies and regulations aimed to address these concerns remains something to watch, and although this may not be an imperative for 2025, the first steps towards building resilience through regulation could start to happen.

- Enhanced Planning: Moves toward harmonisation, especially in centrally operated markets, to pool knowledge and ensure AI and other technologies are developed, deployed and managed in a way that positively contributes to the objectives of secure and cost effective supply.

- A major infrastructure failure: Expect the unexpected. Whether this manifests as a failure due to poor code deployment (as we saw with Crowdstrike) or the exploitation of a vulnerability by a malicious player, this could be the year we see something big happen. Risk managers need to think outside the box and think well ahead, drawing on all their skills, experience and insights to help head off a major failure.

6. Off-shore Wind Sector:

Bad winds are blowing for the off-shore business. A year ago such a prediction might have been considered way left of field and our "wildcard" trend prediction for the year ahead, however, this has been an area we have been monitoring for quite some time and there appears little reprieve in sight as a range of challenges and issues continue to throw the proverbial spanner in the works.

Major providers including Vestas, GE Vernova and Siemens Gamesa have all experienced significant issues with their off-shore businesses.

From quality issues to project execution in highly challenging off-shore locations – which have resulted in rising costs, incurring higher than expected losses, and impacting investor returns.

Given the recent revision of UK government policy which is supportive of on-shore developments, a re-think may be in order. But moving from production of off-shore blades to on-shore blades requires adjustments to manufacturing and therefore, investment (or, to be blunt, more costs).

Conclusions

We are witnessing an increasingly interconnected and complex environment in the energy sector, as reflected in our key trends for 2025.

The intersection of the energy transition and geopolitical fragmentation highlights the complexity of achieving sustainability. The collision of these major global themes has the potential to threaten global stability and derail climate goals and addressing this challenge requires coordinated global efforts to balance sustainability and resilience in the energy economy.

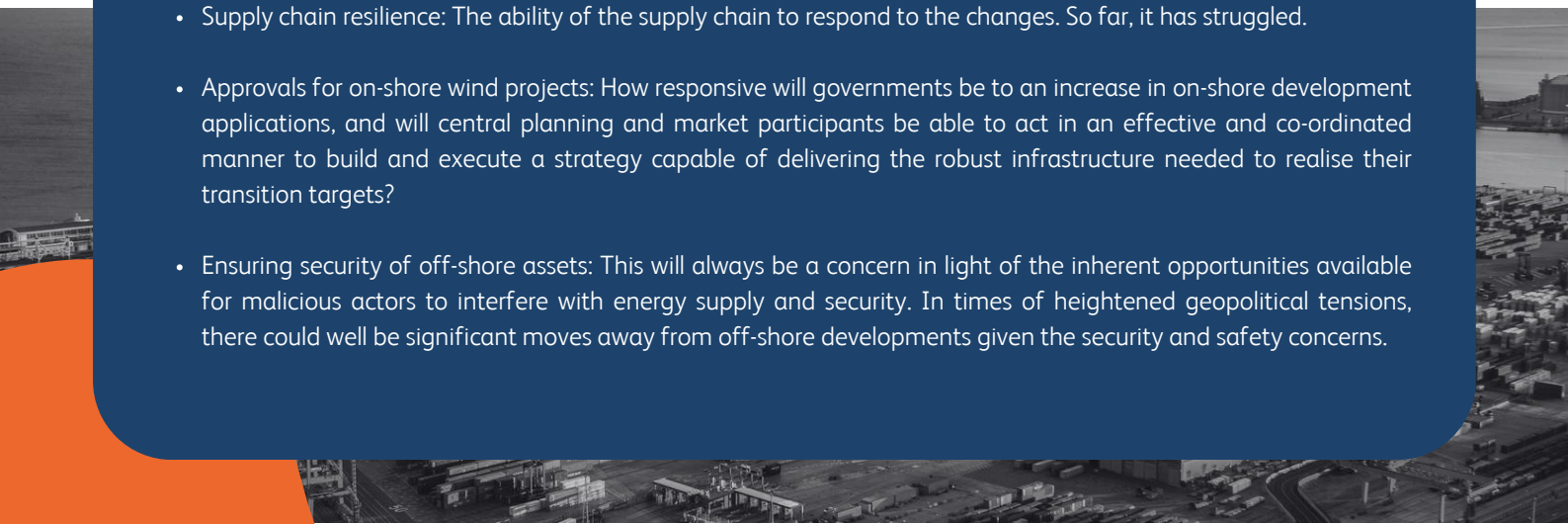
Co-ordinated global efforts are essential to ensure energy becomes a stabilising force, not a source of instability. Without action, the energy transition risks amplifying economic inequality, geopolitical tensions, and climate challenges. The development of regional energy alliances, and strengthened global trade agreements, are crucial to mitigate the risks associated with a range of risks such as resource nationalism.

Supply chain diversification can act as a means of mitigating against the effects of external events and general global / regional uncertainty. Technological innovations like solid-state batteries, sodium-ion alternatives, and advanced recycling aim to reduce dependence on critical minerals. Investors' pursuit of acceptable returns places further pressure on commitments to renewables initiatives, the level of R&D spend on innovative and emerging technologies, electricity grid infrastructure development, and the attainment of mandated global climate and net zero targets.

There are significant opportunities via advancements including moves towards solid-state batteries and investments in HPC-driven grid management, which in turn create new opportunities such as emerging market energy project deployment or recycling of critical minerals as part of a balanced solution to solving the problems of tomorrow.

The big things to keep an eye on include:

- Supply chain resilience: The ability of the supply chain to respond to the changes. So far, it has struggled.
- Approvals for on-shore wind projects: How responsive will governments be to an increase in on-shore development applications, and will central planning and market participants be able to act in an effective and co-ordinated manner to build and execute a strategy capable of delivering the robust infrastructure needed to realise their transition targets?
- Ensuring security of off-shore assets: This will always be a concern in light of the inherent opportunities available for malicious actors to interfere with energy supply and security. In times of heightened geopolitical tensions, there could well be significant moves away from off-shore developments given the security and safety concerns.

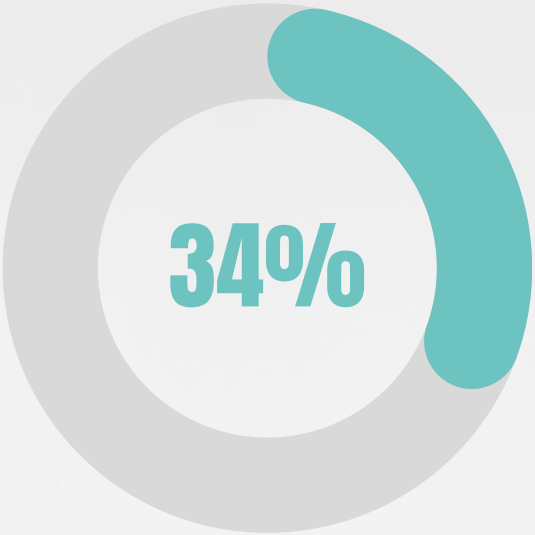


Risk Managers Insights

Our survey revealed several exciting insights from Risk Managers across the world.

We asked risk managers worldwide, how do you expect risk management priorities to shift in 2025 compared to 2024?

- **13%** Increased focus on regulatory compliance and governance
- **28%** Greater emphasis on cybersecurity and resilience
- **14%** Expanded integration of climate and sustainability risks
- **15%** Increased reliance on real-time data for risk mitigation
- **7%** Focus on employee well-being and talent retention
- **23%** Risk management priorities will largely remain the same

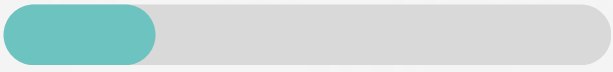


of risk managers feel their organisation does not prioritise risk management in their strategic decision making process

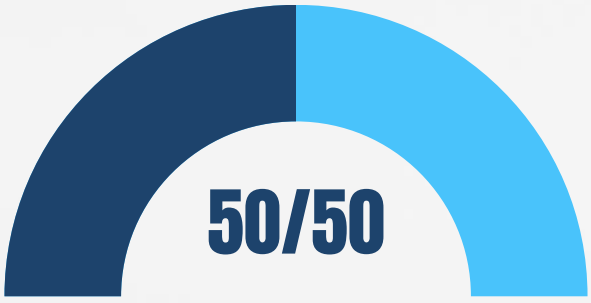
80% of risk managers would rate their organisation's preparedness for managing climate related risks in the next 5 years as above average

57% of risk managers believe they are prepared to respond to another global pandemic

74% of risk managers feel confident that their organisation is prepared to manage future risks associated with AI



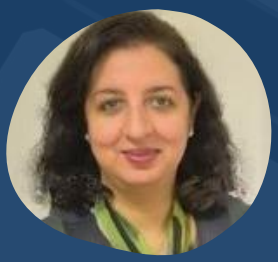
25% of risk managers working in healthcare see business continuity planning as requiring the most significant investment in 2025



when asking risk managers who work in the Energy sector which area they feel will experience the most significant growth or change in 2025 will be, 50% said Cybersecurity and Digital Risks, and the other 50% highlighted Automation Risks.

03

Environmental and Social Governance Special Interest Group



Written by:
Anita Punwani
Director, AMAP Services

Anita Punwani

Anita Punwani CFIRM is a highly qualified risk professional holding the IRM international diploma, MSc in Global Governance & Ethics as well as an MBA and BEng from Imperial College, London. Her experience spans the not-for-profit, public and private sectors.

She joined the IRM in 1998 has supported our institute in relation to education, training, governance and thought leadership. Anita advised UK government officials in the handling of risks to society and the environment for the London 2012 Olympic & Paralympic Games. As Deputy Chair and Non-Executive Board Director of the IRM, Anita was interviewed by the BBC and CNBC during the global pandemic.

Additional Contributors

- Abdul Mohib
- Harriet Milsted
- Lisa Khan

Greater Transparency in ESG

The instability of 2024 will continue to present organisations with many challenges in several respects during 2025; the risk professional will need to consider the full range of challenges the organisation might face in order to support it to successfully manage its risks as well as opportunities into the future. The pressure for greater transparency and accountability to a range of stakeholders will continue in 2025 - and into 2026 - including in relation to managing risks related to modern-day slavery, child labour, equality, diversity and inclusion, as well as health, safety, security and the environment.

In 2024, it became apparent that the simplistic view of 'E', 'S' and 'G' was just that, too simplistic a way of understanding the complexity of risks that the risk professional is now tasked with addressing in the context of the type of challenges the organisation now faces. In this context, it became apparent where organisations are excessively focused on compliance and reporting activities. Whilst organisations have been making changes to their reporting - in part, driven by a desire to meet ever more pressing stakeholder requirements – ESG did see some development from conventional reporting into more mature processes. In relation to the development of ESG reporting going forward, the risk professional will need to support the organisation to ensure it has made a shift in thinking from a traditional mindset to one which reflects the needs of meeting the challenges and requirements of a wider range of stakeholders and society as they manifest. In this regard, risk professionals need to support organisations to be fully transparent in relation to their decision-making. In 2025, many boards will be faced with competing priorities when considering and managing short term versus long term risks. Boards will face short term pressures, including financial ones, and there is a danger that decisions might be made to address these pressures at the expense of proactively identifying, assessing and addressing long term threats and opportunities.

Sustainable Development Goals

Environmental & Social Governance is a key enabler for organisational long-term sustainability. One such issue concerns the exploitation of people and the deprivation of their human rights. The IRM Environmental & Social Governance group concluded its work in the field of modern slavery at the end of 2024 having contributed original thought leadership by adding to the understanding of the complexity of the issue and the role of the risk professional in handling modern slavery risks. This thinking was developed with recognised industry and academic experts in the field namely, Andrew Wallis OBE, CEO of Unseen, and Dr. Bethany Jackson of the Rights Lab at the University of Nottingham. Dr Jackson highlighted IRM's 'active leadership in driving considered thinking in ESG is essential for fostering sustainable business practices.' Andrew Wallis received his OBE for his work in the field including supporting the introduction of the UK Modern Slavery Act. The key learning for the risk professional from this thinking is that the simplistic view of risk management is of limited value in understanding the complexity of risks posed to vulnerable people across the world, including children, where there is the risk of being exploited for profit in global supply chains. The thought leadership also found that there is a complex relationship between the climate crisis and modern slavery risks, based on research conducted by the Rights Lab. In relation to the climate crisis, this is a challenge which is pertinent to organisations working in most sectors and parts of the world. Organisations are increasingly being held to account for the activities they are undertaking and which, for example, may affect water supplies, or affect the vulnerability of areas to wildfires. In relation to managing the risks associated with such challenges, risk professionals need to recognise these as ones not only in relation to the environment but also as social and human rights issues.

The challenge for the risk professional seeking to create a resilient organisation in the context of a rapidly changing environment is the need to understand possible futures in the face of such change.

Extreme weather events are occurring in many regions, such as we saw in the Caribbean in 2024, the like of which had not been seen before at that time of year. The article "Eye of the storm" sets out the opportunities for risk professionals to support organisations in the face of extreme weather events in the 2024 Autumn edition of the Institute of Risk Management's Enterprise Risk magazine.

While regulations may take time to have effect, there is greater consensus across disciplines and sectors that climate change has breached planetary boundaries. Risk professionals are now better placed to support the organisation to take the opportunities as well as responsible action.

With the drive to a more digitalized world, including the use of Advanced Technology and AI, the risk professional needs to support the organisation to build up capabilities in the field of cyber security and data privacy – the risks are becoming more complex.

The challenge for the risk professional seeking to create a resilient organisation in the context of a rapidly changing environment is the need to understand possible futures in the face of such change. In this – indeed in meeting all the challenges set out above – the risk professional needs to be more actively involved in gaining insight in this field, both in terms of gaining competencies as well as in relation to having involvement in professional networks, if they are to handle such matters.

In this respect, the IRM Environmental & Social Governance Group is addressing the role of the risk professional in ensuring greater equality, diversity and inclusion in all organisations. While this issue may be a focus of policy making and compliance in certain respects in many organisations, the need for risk solutions to meet evolving demands means the risk professional needs to lead a more proactive governance arrangement which supports the organisation to identify, assess, manage and monitor these risks and ensure organisational values, sustainability goals, and ethics also support this rights issue. The group is continuing its work with the University of Nottingham in relation to addressing the global challenge of Reducing Inequalities. In 2025, sustainability will continue to be referenced as organisations strive to play their part in helping governments and societies to achieve global goals.

04 Charities Special Interest Group

Written by:
Kathryn Jackson
Risk Manager,
British Heart Foundation

Kathryn Jackson

Kathryn has 15 years of experience in risk management and strategic planning within the charity and not-for-profit sectors and is currently the Risk Manager at The British Heart Foundation, where she manages the ERM framework. She currently serves as the co-chair of the IRM Charity Special Interest Group. This group's aim is to enhance the sector's understanding of risk management best practices, develop practical solutions for sector challenges, and offer opportunities for risk professionals to share knowledge and current practices.

AI and Cybersecurity Threats

2025 brings unique challenges and opportunities demanding strategic foresight and careful management. The Charity Group has identified emerging risks through member consultations.

The amplification of Gen AI represents a significant opportunity for charities, enabling organisations of all sizes to innovate and optimise their resources. Many charities have started to investigate the benefits that AI can bring and are examining use cases that support strategic objectives. There is substantial potential for progress in this field through the utilisation of innovative and creative tools. Failure to adopt these technologies may result in missed opportunities for these organisations. The charitable sector can support workforces by nurturing curiosity and expertise by developing practical guidance and frameworks to work within. This guidance will include iterative procedures that can flex and adapt when technology changes, ensuring potential risk mitigations align with existing data governance procedures, and regularly reviewing mitigation plans. Collaboration with other charities through learning forums and industry events will be crucial for developing awareness and skills in AI.

The Charity Group acknowledges this changing risk landscape and has hosted webinars on risk management and AI. It remains committed to offering training resources and facilitating opportunities for risk leaders to collaborate and exchange best practices.

However, the increased use of AI significantly increases cyber security threats and targeted exploitation from malicious actors. Charities that do not demonstrate security maturity and resilience may experience data losses, regulatory breaches, and a decline in donor confidence.

The integration of AI systems can heighten these vulnerabilities if not managed properly.

To address these risks, charities must understand the evolving risk profile and prioritise cyber security measures. This involves investing in advanced training and awareness programs for their workforce, as well as regularly monitoring outcomes. Security experts both within and outside the charitable sector adhering to industry standards and frameworks will be essential in safeguarding against potential threats.

Workforce wellbeing

The IRM Risk Trends Report of 2024 identified workforce wellbeing as a risk. This issue is expected to continue being relevant in 2025 and is present on many charitable corporate risk registers. Issues such as burnout and staff turnover are contributing factors that complicate efforts to retain and recruit staff.

Charities must continue to prioritise the mental and physical wellbeing of their employees through comprehensive wellness programs, and access to employee support packages.

Although charities have ambitious business planning objectives and utilise resources creatively in operational plans, increased workload pressures are frequently noted in satisfaction surveys. Developing effective talent acquisition and retention strategies is essential. Some charities may not be able to offer competitive salaries and may find it difficult to compete with private sector opportunities. To address this, charities could create appealing benefit packages, including flexible working arrangements where possible and professional development, while fostering a culture of inclusivity and recognition.

Funding resilience

Funding risks remain a challenge for charities in 2025. External economic stress factors, including the cost-of-living crisis, continues to place considerable pressure on the financial sustainability of charitable organisations.

In developing financial resilience, charities must clearly understand their cost base and consider opportunities in diversifying income streams.

It is essential that charities review operational goals, identifying their core deliverables and value add initiatives. Charity risk managers are well placed to support mitigation plans by supporting organisations to model and scenario plan as well as regular horizon scanning to both review opportunities to identify new trends. Charities can enhance their financial and strategic position by collaborating with those that share similar goals.

Changing volunteering delivery model

The volunteer landscape has experienced significant changes following the pandemic. Traditional volunteer pools have diminished, and volunteering demographics have changed.

In response, charities are devising innovative strategies to engage and retain volunteers. Discussions with members of the Charity SIG reveal that innovations such as prioritising flexible volunteering opportunities and offering taster sessions to potential volunteers have been successful in growing volunteering.

Flexible volunteering may be key to addressing the change demands and requirements of volunteers. Charities are developing digital platforms to offer flexible and remote volunteering roles. Charities could leverage technology to adapt to the evolving needs of volunteers. While the landscape of volunteering has changed, it is still important to maintain a strong volunteering culture and deliver a positive volunteering experience. Volunteers can strengthen the delivery of the charitable mission and it some charities, volunteers are key drivers of the delivery model and provide a strong mitigation to operational risks.

Ethical Partnerships in Fundraising

Ethical considerations in fundraising have gained prominence in recent years. Donors and stakeholders are increasingly scrutinising the sources of funding and the ethical implications of partnerships.

It is important that clear ethical guidelines for partnerships and fundraising activities are developed that align with the charity's risk appetite and their ethical investment policy. Charities must conduct thorough due diligence to ensure that potential partners align with their mission and values.

Establishing clear ethical fundraising practices such as transparency in donor communications, respecting donor preferences, and ensuring accountability in the use of funds will enhance credibility and trust.

Conclusion

2025 will require resilience, adaptability, and dedication to charitable missions. By embracing these principles, charities can overcome challenges and seize new opportunities to benefit their recipients.

In 2025, global uncertainty is expected to increase, posing notable challenges for charities. Charity risk professionals must support their colleagues by actively horizon scanning and monitoring the potential impacts on business models.

The IRM Charity Group will play a crucial role in assisting charities to navigate this uncertainty by providing practical solutions and opportunities for sharing best practices.

Charity risk professionals must support their colleagues by actively horizon scanning and monitoring the potential impacts on business models.

05 Cyber Special Interest Group

Written by:
Zhanar Tukeyeva
Risk Management Consultant

Zhanar Tukeyeva

Risk management expert with 20 years of experience, specializing in insurance, enterprise risk management, actuarial analysis, with a focus on helping businesses navigate complex, interconnected challenges.

She has held leadership roles such as Head of Risk at Sukoon Insurance Company and Chief Risk Officer of MENA at AIG, was responsible for supporting the Lloyds syndicate-in-a-box (SIAB) initiative, establishing the ERM frameworks, implementing stress testing for capital management across different countries and jurisdictions, and managing reinsurance credit risk, among other responsibilities.

Cyber Risk in the Modern World

The risk landscape is evolving at an unprecedented pace. Each day's headlines serve as a constant reminder that the future is quickly becoming the present.

It often feels like new risks and response strategies are emerging at every turn. For risk leaders and indeed, all organisational leaders the contours of new opportunities and challenges are already starting to take shape. The most pressing risks are no longer confined to any single domain. Geopolitical instability, security threats, regulatory shifts, cyber risks, and supply chain vulnerabilities are increasingly interwoven with operational risks, including those posed by extreme weather events.

As global power dynamics shift, organisations will need to remain vigilant in the face of rising geopolitical uncertainty, climate disruptions, ethical challenges, and an overwhelming surge of crises.

Here are the key trends and developments that we believe will define 2025 and the years ahead. These emerging dynamics and shifts in the global environment are poised to significantly impact organisations in 2025.

By closely monitoring these major tendencies, organisations can better position themselves to thrive amidst a rapidly evolving and increasingly complex risk landscape.

Supply chain – the interconnectedness of the world

Technologies such as IoT and blockchain play an essential role in tracking and managing supply chain risks in real-time. These smart devices, embedded with sensors, communication tools, and computing power act as constant points of monitoring and enforcement. This shift will enable organisations to detect risk events, gain valuable insights, and even take immediate action within their operational environment. The result will be a dynamic, always-on risk management system that ensures a rapid and informed response to emerging threats.

While IoT and blockchain technologies will enhance real-time supply chain risk management, they may also introduce new types of cyber risks. As more devices become interconnected, the attack surface for cybercriminals expands, providing multiple entry points for potential breaches.

The vast amount of data exchanged between IoT devices could be intercepted or manipulated, increasing the risk of data theft or tampering. Furthermore, as blockchain becomes a key tool in tracking transactions, its complex algorithms may be vulnerable to targeted attacks, such as smart contract exploits or 51% attacks. The reliance on these technologies for risk management means that a failure or compromise in any connected device or blockchain system could cascade across the entire network, leading to significant disruptions or financial losses. In essence, while these technologies offer improved efficiency, they also require organisations to evolve their cybersecurity strategies to protect against an increasingly sophisticated range of digital threats.

As more devices become interconnected, the attack surface for cybercriminals expands, providing multiple entry points for potential breaches.

Borderless World – Fluid Economies.

Advances in technology are dissolving traditional physical and regulatory barriers, enabling a world where individuals and organisations can interact, innovate, and thrive beyond geographic constraints. Freelance platforms and the gig economy expand cross-border work opportunities, while telemedicine and online education make essential services universally accessible.

The rise of remote work, smart cities, and global financial systems opens up new markets, but also increases vulnerabilities.

Cyber-attacks have also moved more toward targeting homes and private individuals (where security tends to be weakest).

That will also create new cybersecurity markets.

The prediction that cyber-attacks targeting homes and individuals will rise as part of risk trends for 2025 is based on observable patterns, current incidents, and technological advancements:

1

Data from Recent Reports and Incidents

Reports from cybersecurity firms and global risk assessments highlight the shift toward targeting individuals. For example:

- IoT Botnet Attacks: Mirai malware, which has evolved to target smart home devices, disrupting internet services.
- Phishing Campaigns: The FTC reports significant increases in phishing targeting individuals for financial fraud. In the first quarter of 2024 alone, consumers reported losing $20 million to scams involving criminals impersonating government officials and demanding cash payments.
- Exploitation of Remote Work Vulnerabilities: Attacks like ransomware via unsecured remote desktop protocols are on the rise.

2

Additionally, as smart cities grow and more devices become connected, the risk of IoT exploitation increases. Poorly secured devices such as surveillance cameras and smart meters could be targeted for cyberattacks, as seen in previous botnet attacks. Many smart home devices lack proper safeguards, and personal networks often use outdated protections, making them prime targets for cybercriminals. Emerging threats, including ransomware, phishing, and IoT botnet attacks, highlight the urgent need for stronger cybersecurity at the individual level.

3

Geopolitical and Economic Drivers

As global tensions rise, state-sponsored attackers and organised cybercriminals increasingly target private individuals to create widespread disruption or financial gain.

With remote work, global workforces present a bigger attack surface. Hiring across borders means dealing with contractors and employees from jurisdictions with different data protection laws, raising the risk of data leaks, whether accidental or malicious. Cross-border digital nomad lifestyles could expose individuals to jurisdictional gray areas, complicating data privacy and cybersecurity protections. AI-powered attacks, like deepfakes and automated phishing, will challenge authentication systems and decision-making.

The evolution of financial systems and the push for Central Bank Digital Currencies (CBDCs) bring additional risks. Decentralized finance (DeFi) platforms are susceptible to hacks and fraud, as demonstrated by the Poly Network hack in 2021, where $610 million was stolen. The lack of consistent regulatory oversight in cross-border transactions further exacerbates the risk of money laundering and cyber fraud.

Social media and virtual communities, while providing global connectivity, also foster the spread of disinformation and cyber risks. Deepfake technology and state-sponsored misinformation campaigns can manipulate public opinion and compromise personal security.

Moreover, as space commerce grows, so does the potential for cyberattacks on satellite systems, which are crucial for communication, navigation, and military functions. Governments worldwide are increasingly leveraging commercially available technologies to enhance resilience and maintain a competitive edge in conflicts.

Solutions like commercial satellite communications and advanced computing offer rapid deployment of innovative capabilities at scale for both military and intelligence applications. However, dual-use commercial services—those serving both civilian and military needs—are becoming prime targets for state-sponsored cyberattacks.

Adversaries are likely to exploit these systems to disrupt, degrade, or deny access during conflicts, impacting both military operations and civilian infrastructure reliant on the same technologies. For instance, commercial satellite systems supporting communication, navigation, and remote sensing are particularly vulnerable to cyberattacks, with potential cascading effects on critical civilian systems and services.

This highlights the growing intersection of cyber threats and dual-use technologies in modern conflicts.

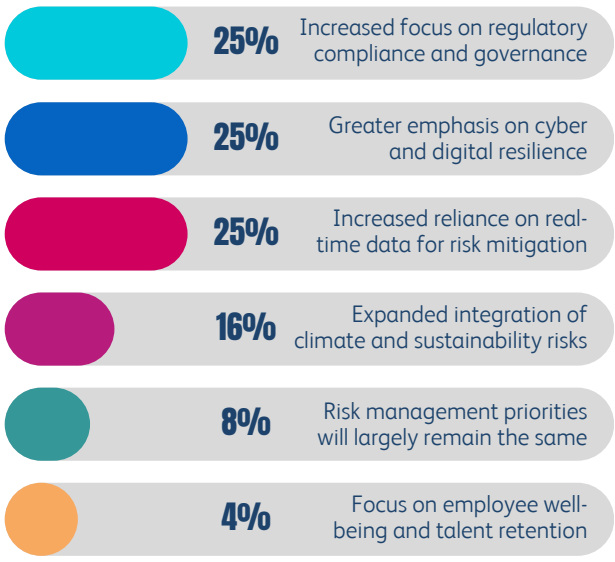
Cybersecurity risks extend to e-commerce and digital supply chains, which can be disrupted by attacks like the SolarWinds breach. Furthermore, the challenges of data sovereignty increase as sensitive customer information is stored in countries with weaker data protection laws.

Finally, the integration of AI and machine learning into workflows presents risks like algorithmic exploits and data privacy violations. These technologies, while enhancing business operations, also expose systems to potential manipulation and breaches.

These examples illustrate how digital and physical risks are increasingly intertwined. As technology continues to evolve, organisations must develop more robust cybersecurity strategies to address these new and emerging threats.

As digital ecosystems grow, new challenges will emerge, including the need for stronger encryption, cross-border regulatory frameworks, and proactive AI-based defenses to address evolving cyber threats. The global shift toward a borderless world must be met with equally advanced strategies to safeguard individuals, organisations, and infrastructure.

Practitioners working in Cyber expect their priorities to change in 2025, in the following ways:


25%
Increased focus on regulatory compliance and governance
25%
Greater emphasis on cyber and digital resilience
25%
Increased reliance on real-time data for risk mitigation
16%
Expanded integration of climate and sustainability risks
8%
Risk management priorities will largely remain the same
4%
Focus on employee well-being and talent retention

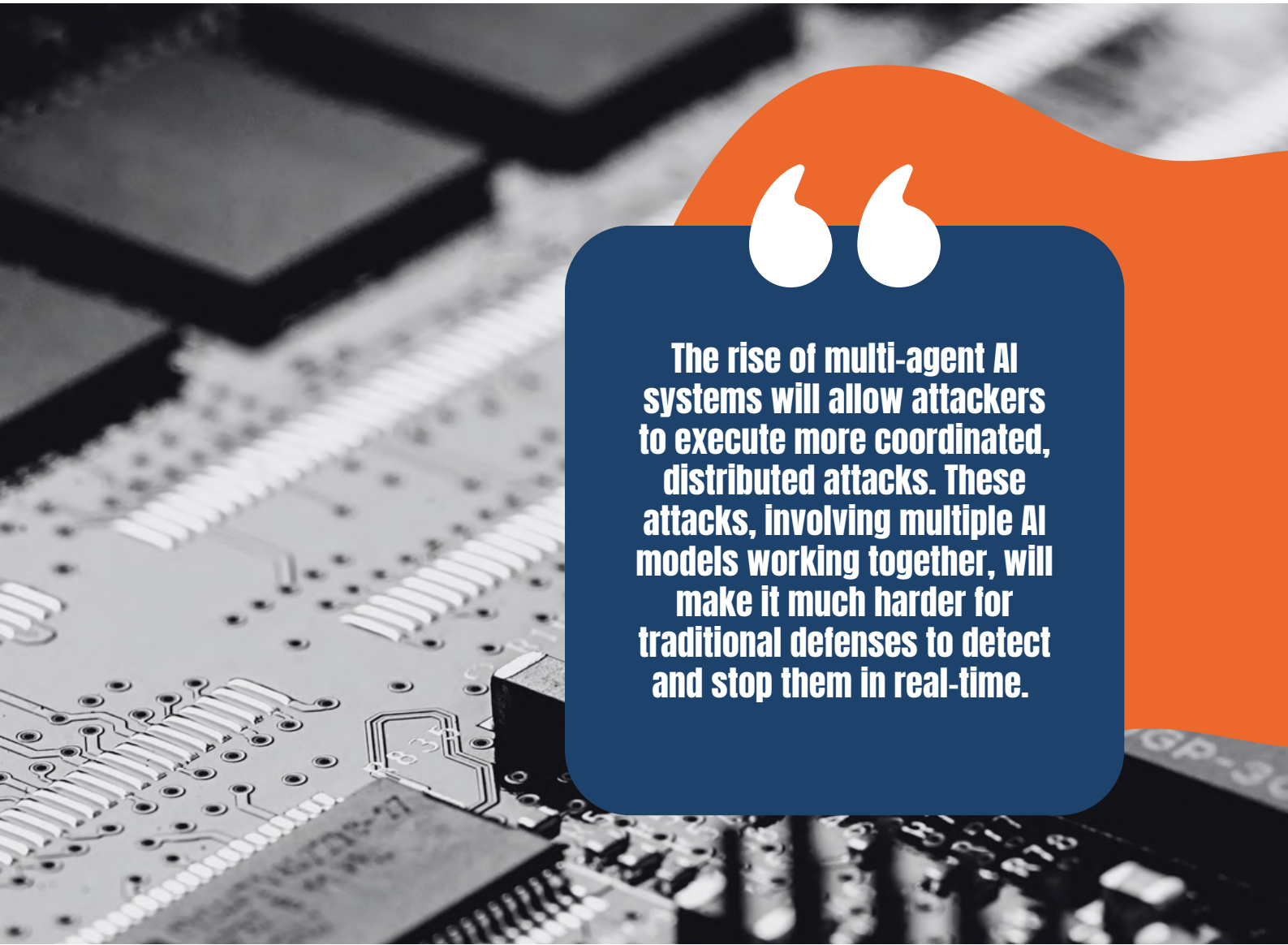
Big Tech – a dependency risk

The increasing reliance on a handful of Big Tech companies has created a new dependency risk for the global economy. These companies, providing an array of interconnected services—such as search engines, social media platforms, cloud services, and even generative AI—have become central to the functioning of both businesses and daily life.

While Big Tech firms invest in redundancy measures to safeguard their infrastructure, such as geographically dispersed data centres, the potential for large-scale disruptions remains a critical concern. Whether due to human error, natural disasters, or cyberattacks, a prolonged failure of these services could have wide-reaching consequences, affecting not just businesses but also governments and individuals globally. As the complexity of the risk landscape grows, so does the challenge of managing these interconnected dependencies. A failure by one company could ripple through various sectors, making risk management more intricate.

Cybersecurity risks will continue to evolve alongside this growing dependency. With increased interconnectivity, hackers may target vulnerabilities across multiple platforms simultaneously, potentially exploiting weaknesses in cloud services or data-sharing networks.

The rise of AI in these services further amplifies the risk, as cybercriminals may leverage AI to launch more sophisticated, automated attacks. The rise of multi-agent AI systems will allow attackers to execute more coordinated, distributed attacks. These attacks, involving multiple AI models working together, will make it much harder for traditional defenses to detect and stop them in real-time. Furthermore, concerns about social media's role in political polarisation, data privacy, and the influence it has on societal behaviors add another layer of complexity to this risk landscape, requiring robust and adaptive risk management strategies. As these technologies evolve, so too must our understanding of the cyber threats that accompany their growth.

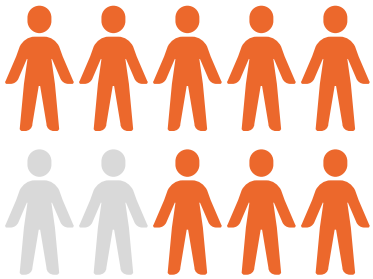


The rise of multi-agent AI systems will allow attackers to execute more coordinated, distributed attacks. These attacks, involving multiple AI models working together, will make it much harder for traditional defenses to detect and stop them in real-time.

Quantum Computing

Quantum computing, once seen as a distant possibility or the stuff of science fiction, is rapidly becoming a reality. Much like artificial intelligence in 2015—fascinating but not yet mainstream—quantum technologies are poised to transform the landscape of computing and knowledge.

In just a few years, quantum computing could be as integrated into our systems and applications as AI is today, unlocking unprecedented levels of understanding and capability. As these technologies grow in scalability and reliability, advancements in quantum computing, communication, and sensing will revolutionise various domains. Immersive experiences, powered by quantum-driven innovations, will become so advanced they may blur the lines between virtual and physical realities.



8/10 practitioners anticipate that the demand for risk management professionals with cybersecurity skills will increase significantly in 2025.

In November 2024, scientists from China and the US achieved a remarkable breakthrough in quantum computing by creating a time crystal using a quantum processor. A time crystal is a unique state of matter that defies typical physics by exhibiting a constant "ticking" motion without using energy. First proposed by physicist Frank Wilczek in 2012, the idea was initially met with skepticism. However, experiments have since proven its existence in various systems.

This discovery is significant because time crystals could help solve key challenges in quantum computing, such as improving accuracy and creating stable quantum memory. It also shows how quantum computers can be used to test complex ideas in physics. Time crystals might play a big role in the future of quantum technology, opening doors to new possibilities and applications.

Current public-key cryptographic systems underpin the security of sensitive online communications, such as banking, email, and website access. However, the advent of quantum computers capable of performing complex calculations at unprecedented speeds would render these systems vulnerable, effectively breaking their cryptographic protections.

Even traditional shared-key cryptosystems would not be immune, as their security would be weakened—essentially halving their current strength, although increasing key lengths will mitigate this. This highlights the urgent need to develop quantum-resistant cryptographic solutions to safeguard digital communications in a post-quantum era.

There is absolutely no certainty regarding how correct or incorrect these predictions will turn out to be. Many of the near-term predictions are, however, already emerging, or based on patterns that have continued for many decades. The most amazing thing about technology is that we no longer need to consider if something is possible. It is now possible to create almost anything.

The rise of quantum computing introduces unique risks that go beyond traditional computational challenges. One major concern is the risk of incorrect results. Quantum computers operate using qubits, which are highly sensitive to external disturbances. If the system is not properly maintained under specific conditions, errors can occur in calculations, leading to unreliable outputs.

Another challenge is the multiplicity of results and outcomes. Quantum computing leverages superposition, where qubits can represent multiple states simultaneously. While this offers immense computational power, interpreting these multiple potential outcomes can be complex, requiring specialized algorithms and expertise to identify the correct solution. Quantum systems must operate in controlled environments to prevent decoherence, a phenomenon where qubits lose their quantum state due to interaction with their surroundings.

As quantum computing advances, addressing these risks will be critical to ensuring its reliability and widespread adoption in industries like cryptography, finance, and artificial intelligence.

Complex World and Cyber Risk interconnectedness

Organisations relying on past successes as a guarantee for future performance risk failure by ignoring the need to adapt to a rapidly changing environment.

The modern world faces constant disruptive change, driven by interconnected activities and events that accelerate the pace of transformation. As a result, decision-making has become more complex, while many existing models used in education, workplaces, or governance are not equipped to handle the current level of complexity and uncertainty. Adapting to these dynamic conditions requires updated approaches and innovative thinking.

Risks today are not isolated. As the world becomes more interconnected and complex, the relationships between various risks grow stronger, with cyber and digital risks standing out as prime examples. Events like pandemics and the impacts of climate change influence the digital landscape by altering the environments in which technology operates.

These changes introduce new vulnerabilities and heighten existing risks, showcasing how traditional and digital threats are increasingly intertwined. Here are some examples of how these risks are expected to intersect with other domains.

Cyber Risks and Climate, Environmental Risks

As climate change drives more frequent and intense natural disasters, the overlap between physical and cyber risks is becoming a critical concern for 2025. While hurricanes or other natural disasters are not uncommon, the combination of such an event with cyberattacks timed to exploit the disruption is less frequent but increasingly possible due to the growing complexity of cybercrime.

Consider the cascading effects of a Category 4 hurricane striking a coastal region. Beyond the immediate physical damage—power outages, flooding, and structural devastation—such an event cripples critical digital infrastructure, including cloud data centers relied upon by finance, healthcare, and other industries.

This disruption causes significant operational downtime, exposes vulnerabilities in digital backup systems, and delays recovery efforts. Cybercriminals capitalise on this chaos, launching ransomware attacks and exploiting disaster recovery gaps. Phishing schemes disguised as emergency alerts or offers of aid further prey on affected organisations and individuals, compounding the crisis.

The combined impact is severe: organisations face operational shutdowns, compromised data, and loss of trust. Businesses, already under pressure to restore physical systems, are forced to battle simultaneous cyber threats. This trend highlights the urgent need for integrated risk strategies that address both physical and digital vulnerabilities, ensuring resilience in an era of interconnected risks.

Cyber risk and Geopolitical, Economic factors

Digital and cyber risks are becoming increasingly intertwined with geopolitical, economic, and technological factors, creating complex challenges for organisations. The overlap of cyber risk with geopolitical and economic factors is intensifying, amplifying vulnerabilities that span across businesses, governments, and economies.

These risks can lead to significant disruptions, from espionage and data theft to more destructive actions like targeting critical infrastructures, such as power grids, healthcare systems, and manufacturing facilities. For example, cyber risks threaten essential systems like air traffic control, which depend heavily on interconnected technologies for safe and efficient operations.

To mitigate these growing threats, organisations must adopt coordinated strategies that promote resilience and ensure the ability to recover from potential disruptions. Emerging technologies, such as generative AI, intensify these risks by enabling malicious actors to exploit sensitive information or tools that could threaten sectors like defense or energy. This underscores the need for organisations to integrate both digital and physical risk management frameworks to defend against evolving global security challenges.

Given the increasingly global and interconnected nature of cyber risks, businesses must align their strategies with geopolitical trends and proactively protect their infrastructures across borders.

So, how can we start adapting to an increasingly complex world? For this case foresight with system thinking is needed because the complexity rises.

As complexity in the modern world increases, foresight coupled with systems thinking is essential for navigating challenges effectively. Unlike linear thinking, which breaks a puzzle apart to look at each piece, systems thinking pieces together the puzzle to look at the whole picture while also examining how those parts interact within the larger context, offering a more comprehensive perspective.

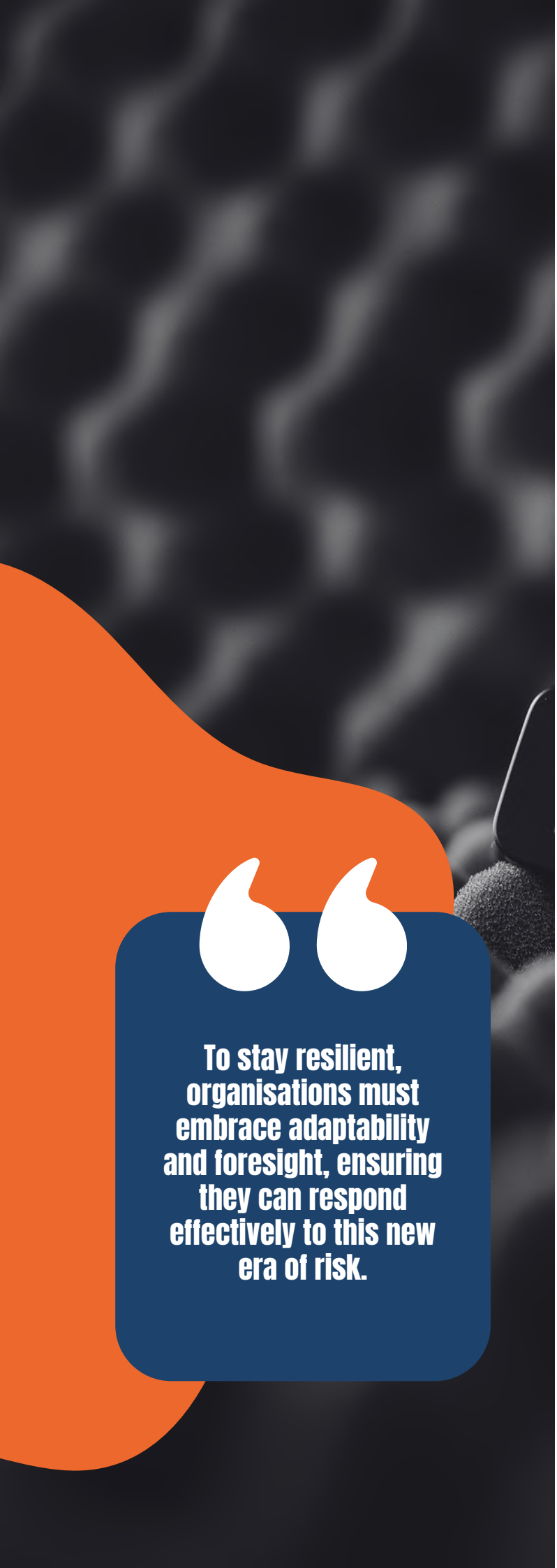
It emphasises understanding not only the components of a system but also the processes and relationships that connect them. Systems thinking recognizes the existence of different types of systems—some complicated, where problems can be resolved through analysis and expertise, and others complex, where outcomes are unpredictable due to dynamic interdependencies. Despite its value, many struggle with this holistic approach, often prioritizing short-term gains over addressing intricate, long-term challenges. By shifting focus toward interconnected systems and their broader contexts, organisations and individuals can build resilience and adaptability in an increasingly interconnected world.

In order to think in the long term and of the implications of our actions, we need to have an open mind and stretch our imagination.

Futures thinking is a way of thinking about what's possible more deeply, honestly and strategically. It is as much an art as a science. You will need to rely on creativity, intuition and insight, as well as research and analysis.

Futures thinking contrasts with forecasting, and forecasting models. Most forecasting models look at historical trends and, with various degrees of sophistication, attempt to project them forward. But the models are based on a fixed view of how the overall system operates, so their reliability starts to break down over the longer term as the world changes. In order to achieve such foresight, a number of tools and techniques have been developed over the years with which a skilled practitioner can attempt to reduce uncertainty. These tools include trend analysis to project the past into the future, scenario planning to understand the world given a particular set of parameters, and stress testing to better identify the weak links within our systems.

However, it is horizon scanning which has become the buzz word of the modern organisation. Horizon scanning can be a good technique for people to look at complexity, challenge assumptions and review multiple ways that events could unfold, in order to increase the resilience and reliability of their organisations.



> **To stay resilient, organisations must embrace adaptability and foresight, ensuring they can respond effectively to this new era of risk.**

Traditional methods often lack the sophistication to address modern risks like digital vulnerabilities, systemic financial risks, or climate-induced disruptions. Emerging tools such as artificial intelligence, scenario-based modelling, and quantum computing are increasingly being adopted to navigate this complexity.

The future of risk management is evolving, driven by the emergence of new types of risks and the transformation of traditional ones. Companies will need innovative tools and analytical approaches to navigate this changing landscape. Unlike conventional risks, these emerging challenges often represent a complex interplay of interconnected and symbiotic threats, reflecting the growing complexity of global systems.

To stay resilient, organisations must embrace adaptability and foresight, ensuring they can respond effectively to this new era of risk.

As risks transform, the ability to forecast them may become increasingly short-term due to rising uncertainties and the multiplicity of potential outcomes. As uncertainties grow due to rapid technological advancements, shifting geopolitics, and environmental changes, the ability to predict risks far into the future diminishes.

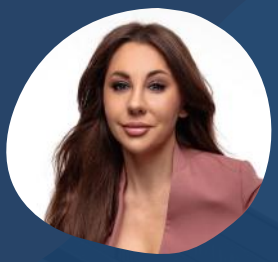
Decision makers are increasingly relying on dynamic, real-time risk assessments.

The development of future trends will likely hinge on where human attention and focus are directed, as collective consciousness shapes the priorities and trajectories of our interconnected world. As we face complex global challenges—ranging from digital transformation to climate change—the priorities we set today will shape the world of tomorrow.

The collective consciousness and collective action of global societies will influence how effectively we address emerging risks and harness new opportunities.

By steering focus toward collaboration, innovation, and resilience, we can ensure that our interconnected world evolves in a way that prioritises sustainability, security, and societal well-being. Where we choose to direct our attention will define the trajectory of these evolving trends and their impact on our future.

06 Financial Services Special Interest Group



Written by:
Anastasia Rackovska
Head of Enterprise Risk Management, Paynt Group

Anastasia Rackovska

With more than 10 years of experience in the financial industry, transitioning from managing Risk Department operations—covering customer onboarding, due diligence, compliance, transaction monitoring, and credit risk assessment—to leading Enterprise Risk Management, with a focus on company-wide risk strategies and effective oversight across all areas.

JOIN

Resilience isn't just a buzzword

In the fast-paced world of finance, resilience isn't just a buzzword - it's essential for survival. Technology is pushing boundaries, financial instruments are becoming increasingly complex, and client expectations are higher than ever.

At the same time, institutions are being pulled in opposite directions: regulators demand stability, while competition and customers push for faster, smarter, and more innovative solutions. It's a race to keep up, adapt, and thrive in an industry that never stands still. As we look to 2025, new challenges and opportunities lie ahead to shape the future of finance.

Mind the Gap: Building Talent for Tomorrow's Industries

The rapid pace of innovation in areas like ESG, AI, and cybersecurity has created a skills gap in the financial sector.

In 2025, institutions may struggle to recruit and retain talent with expertise in these fields, hampering their ability to adapt to new challenges effectively. Investments in workforce upskilling and strategic partnerships will be critical.

Digital Currency and Blockchain

Central bank digital currencies (CBDCs) are becoming a reality, with several countries launching or piloting their own in 2025. This development, coupled with the growing use of blockchain technology, introduces new operational and cybersecurity risks.

Financial institutions must prepare for potential fraud schemes, interoperability challenges, and the need to upgrade infrastructure to handle digital currency flows securely.

Beyond these operational concerns, the environmental implications of blockchain technology also warrant attention. Its impact on ecology and resource consumption is significant. Energy-intensive blockchain processes, especially proof-of-work mechanisms, contribute to carbon emissions and demand substantial resources. To mitigate this, stakeholders must balance innovation with sustainability by investing in greener, resource-efficient technologies.

AI Regulation and Ethical Challenges: A Double-Edged Sword

Artificial intelligence (AI) continues to evolve, serving as both a game-changer and a battleground in the financial sector. Institutions use AI to streamline operations, personalise customer experiences, and detect fraud faster than ever. At the same time, fraudsters are leveraging AI to enhance their scams, creating a constant race: Who can use AI more effectively—financial institutions or fraudsters?

On one side, fraudsters are using AI to generate realistic phishing attacks, bypass biometric authentication, and create deep-fake identities, making their scams harder to detect. Machine learning models in the wrong hands can quickly identify vulnerabilities in financial systems, often outpacing the ability of institutions to respond.

On the other side, AI is proving indispensable in fighting back. In the UK, Mastercard's AI-powered Consumer Fraud Risk (CFR) solution has become a powerful tool against Authorised Push Payment (APP) fraud.

By analysing payment data in real-time, it evaluates transaction patterns, account details, and connections to known scams.

This system allowed banks to intercept fraudulent transactions before completion, reducing fraud losses by £48 million - from £389 million to £341 million in 2023. Without AI's ability to process and analyse vast amounts of data instantly, such outcomes would have been impossible. As AI systems advance, so do the tactics of bad actors, creating an arms race between innovation and malfeasance.

Recognising the challenges and opportunities of AI, governments around the world are stepping in to regulate its use. The European Union's Artificial Intelligence Act categorises AI systems by risk levels and establishes strict requirements for high-risk applications. The United Kingdom is adopting a pro-innovation framework guided by principles such as transparency, fairness, and accountability.

The United States, through international summits and local initiatives, is shaping AI governance, while China enforces strict regulations on algorithmic recommendations and deep synthesis technologies. These global efforts aim to ensure AI is used ethically and responsibly, addressing its risks while fostering innovation.

However, the impact of AI is not confined to fraud prevention. Its development and deployment also carry significant ecological consequences, raising ethical questions. AI systems require vast amounts of electricity and cooling resources, creating a substantial carbon footprint, particularly in data centres reliant on non-renewable energy.

As AI adoption grows, the strain on global energy infrastructure will prompt discussions about sustainability. Who will harness AI better? Can regulators and firms keep pace while addressing the environmental cost of innovation?

Climate Transition Risks: Still in the Spotlight for 2025

As economies accelerate their shift toward low-carbon models, financial institutions face heightened transition risks in 2025.

Clients in high-emission industries are under increasing pressure from stricter regulations, such as carbon taxes, and shifting market preferences.

Financial institutions are also addressing these challenges. Some have ceased investments in new bonds from oil and gas exploration companies, reflecting a strategic move away from high-carbon industries to mitigate portfolio risks and support sustainability goals. Others have committed to achieving net-zero emissions by 2050, integrating environmental due diligence into credit assessments and setting greenhouse gas reduction targets for key sectors.

Additionally, climate scenario analysis methodologies are being developed to measure the impact of transition risks on portfolios, enabling more informed risk management strategies.

To mitigate transition risks, financial institutions must integrate climate considerations into credit risk assessments, identify vulnerable clients, and adjust lending criteria to favour low-carbon industries. Failure to act could lead to financial instability, reputational damage, and regulatory penalties.

These proactive measures not only safeguard financial health but also position institutions as leaders in sustainable finance, ensuring resilience in a rapidly greening economy.

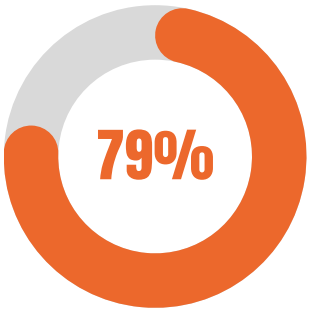
Geopolitical Risk

After a few turbulent years marked by the COVID-19 pandemic and ongoing conflicts in Eastern Europe, the Middle East, and Asia, the world is eager for stability, brighter prospects, and renewed economic growth. However, one significant uncertainty continues to loom large: geopolitical tensions.

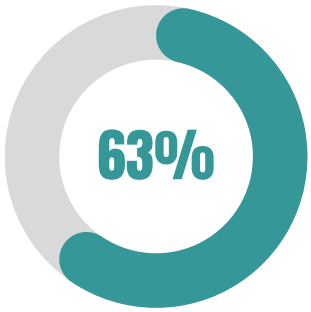
In 2025, geopolitical tensions will heighten risks such as supply chain disruptions and market instability. Conflicts or sanctions in key regions could limit access to resources, disrupt trade, and increase energy costs, posing challenges for financial institutions. These disruptions elevate credit risks for businesses reliant on fragile supply chains or volatile energy markets. Changes in trade policies or sanctions could strain liquidity, raise costs, and trigger loan defaults or asset devaluation.

Amid these challenges, the global spread of innovation is reshaping strategies as companies increasingly move to markets that offer greater stability and fewer regulatory barriers. For example, firms are shifting operations from regions like the UK, where regulatory complexities and stringent compliance requirements may stifle growth, to markets like the US, which are seen as more business-friendly and conducive to innovation.

This trend reflects a strategic pivot as companies seek environments that balance oversight with opportunity, allowing them to adapt more effectively to global uncertainties. While stability is hoped for, geopolitical uncertainties and market dynamics will continue to drive businesses to reposition themselves, prioritising resilience and agility in an ever-changing global landscape.



of risk professionals from the financial services industry anticipate the demand for qualified risk experts will increase in 2025.



risk professionals in financial services believe the industry has enough skilled professionals to meet their industry's needs.

07 Climate Change Special Interest Group

Written by:
Martin Massey MIRM
Managing Director,
OneRisk Consulting Ltd

Martin Massey MIRM

Martin has worked in the risk management profession for over 30 years for some of the leading global insurance and risk consulting firms including Swiss Re; AIG and Enstar Group and within risk consulting practices of Marsh, Aon and WTW. He is a leading practitioner in Enterprise Risk management and was a Chief Risk Officer for a Lloyds Syndicate in London and approved by the Bank of England as an (SMF4).

- In 2020 he set up his own company, OneRisk Consulting Ltd and became Chair of the IRM Climate Change Group. He has been advising a number of leader organisations including Milliman and Moody Analytics and is currently a strategic advisor to Howdens Group's climate risk and resilience team.
- In 2022 he published in December 2022 "Climate Change Enterprise Risk Management: A practical guide to reaching net zero goals" which was endorsed by the IRM.
- In 2023 he became an academic lead at Cambridge University, where he designed a leading globally recognised ESG risk management course for executives.
- In 2024 Martin was named IRM Risk Management Leader of the Year at the CIR award for his contribution to climate change and ESG risk management.

Additional Contributors:

- Christine Page
- Jerry Flechais
- Felipe Palacios
- AJ. Ahad
- Wajahat Khawaja
- Rose Chemutai

Introduction

The world economic forum (WEF) have just issued their 2025 global risk report in which extreme weather events are ranked as the #1 risk for the next 10 years, they state that "the effects of climate change driven extreme weather events are being felt across the world and often hit the poorest communities the hardest. Global heat records continue to be broken".

The burden of climate change is becoming more evident every year and is evidenced by the Asia heatwaves in Indonesia, Europe, the Brazil flooding; Canadian wildfires, and hurricanes Helene and Milton. They state Green transition must centre on "super-pollutants" including black carbon, methane, HFC's and tropospheric ozone. The reason for this is because super-pollutants account for 45% of near-term global warming.

Organisations continue to take positive steps to meet regulatory and business requirements and embed climate change into their enterprise risk management frameworks and business processes. Focus areas in 2025 continue to be developing best practices in transition plans and reporting and monitoring of climate change risks including scope 3 emissions as well as developing improved controls particular in respect to adaptation and resilience to ongoing threats from physical risks of climate change, risks through a range of innovative risk management solutions such as use of parametric or event driven insurance risk transfer to support ever increasing areas of under or uninsured risks.

The Group committee have set out five main macro risk themes, and that risk managers should focus on in terms of risk trends and predictions in 2025 in the context of managing and mitigating their risks in their business. Some of the major climate risk trends that were included in the seminars that we conducted in 2024 which we expand on in this year's risk trends report.

Physical Risks

1. Increase in flash floods
2. Increase in severe droughts leading to water scarcity

2024 has been another year of extreme weather and a recent study by Swiss Re estimates NatCat losses of $120bn USD in 2024, the second highest in recorded history. Many of these are macro, climate related Natural catastrophes that include an increased propensity for flash floods that we saw in the fall of 2024.

These affected several European countries, including Spain, Austria, and Italy.There are, of course, several ongoing emerging climate risks that we have covered in previous years' reports including wildfires and we have recently witnessed the LA wildfires in January 2025.

Transition Risks

3. Inability to attract green skills talent
4. Failure to meet climate emissions targets
5. Enhanced decarbonising innovations including carbon capture and storage

It is worth mentioning that since we developed the list if transition risks Trump has been reflected and the US has just pulled put the Paris Agreement which is likely to lead to significant environmental implications not least in the potential to increase carbon emissions and weaken global climate action.

Physical Risks - Increase in flash floods

Flash floods are becoming more frequent and severe as a result of climate change, with intensified rainfall and storm events overwhelming infrastructure and causing widespread disruption.

In the fall of 2024, several European countries, including Spain, Austria, and Italy, experienced catastrophic flash floods following Storm Boris, which dropped a month's worth of rain in just 24 hours.

The storm caused significant property damage and loss of life, with Valencia receiving more than an entire year's worth of rainfall in only eight hours. Flash floods occur when rainfall exceeds the ground's capacity to absorb or drain water due to inadequate urban infrastructure.
It also often occurs in dry areas because parched soil tends to repel water rather than allow it to soak in.

As global temperatures rise, the atmosphere can hold more moisture, driving heavier rainfall and more frequent flash floods. This is particularly challenging for older cities with outdated drainage systems that cannot cope with such extreme events.

The 2024 Valencia floods alone led to over 138,000 insurance claims, with losses estimated at €3.5 billion.

> **Governments, businesses and organisations must invest in resilient infrastructure, improve early warning systems, and secure insurance coverage.**

This was caused by a DANA (a Spanish acronym representing a high-altitude, cut-off low-pressure storm system), where a cold air mass broke from the jet stream, colliding with warm Mediterranean air and forming a slow-moving storm with heavy rainfall. Such events highlight the growing financial and operational risks associated with flash floods, particularly as climate change increases the severity of such flooding events due to warmer temperatures that allow the atmosphere to hold more moisture making rainfall events more unpredictable.

Governments, businesses and organisations must invest in resilient infrastructure, improve early warning systems, and secure insurance coverage. However, high-risk areas face challenges in obtaining insurance, as insurers may withdraw from these markets, as seen with wildfires in California. Governments play a critical role, with initiatives like Italy's new law requiring companies to buy flood insurance starting in 2025, and Spain's Consorcio de Compensación de Seguros (CCS) providing support in flood events. Other state-backed insurance programs, such as the UK's Flood Re and France's CCR, are essential for managing financial risks.

Due to flash floods, there is also a risk of supply chain disruption due to extreme weather events, shortages of natural resources, price fluctuations in commodity prices etc.

In summary, flash floods are a significant and growing threat due to climate change. Risk managers must consider the increasing likelihood of such events in their risk planning, focusing on infrastructure upgrades, disaster preparedness, and comprehensive insurance solutions.

Increase in severe droughts leading to water scarcity

Droughts describe a lack of water caused by an extended period of weather without sufficient rainfall. Severe droughts can have an impact on the ecosystem, agriculture and the wider economy and increase the risk of wildfires.

Climate change is a primary driver of more intense and frequent droughts. Rising global temperatures lead to higher evaporation rates, decreasing water availability.

Altered rainfall patterns also contribute to reduced water supplies, as some regions experience prolonged dry spells while others face irregular, intense rainfall. Human activities such as overextraction of water for agriculture and poor water management further exacerbate the situation. Deforestation and land degradation also reduce the land's ability to retain water, increasing vulnerability to drought. Drought also forces human migration and as per World Bank's Groundswell report, Climate change, an increasingly potent driver of migration, could force 216 million people across six world regions to move within their countries by 2050.

The California drought (2011-2017) is a prime example of how climate change can increase the severity of water scarcity. It was one of the longest and most intense droughts in the state's history, leading to widespread crop failures, rising food prices, and severe economic losses in agriculture. Similarly, Cape Town's 2011-2017 drought, exacerbated by lower-than-usual rainfall and high evaporation rates, brought the city to the brink of "Day Zero," where water reservoirs were expected to run dry, forcing drastic measures such as water rationing. These examples underline how climate change can increase both the likelihood and the severity of droughts, threatening water supplies and destabilizing local economies.

It is important however to recognise that on average, the UK experiences a drought every five to ten years, with the South East suffering most as it has the highest population and demand for water, as well as the lowest levels of precipitation.

As water scarcity affects more regions, businesses must adopt water-saving technologies, improve infrastructure, and develop drought-resistant strategies. Organisations should actively engage in water stewardship—working collaboratively with governments, communities, and other stakeholders to manage shared water resources—can help mitigate the risks of water scarcity. Risk managers should incorporate these considerations into their planning through developing robust water management strategies, scenario testing and stress assessments to prepare for potential disruptions.

Insurers, in turn, must adapt their policies and pricing models to account for the increasing risks of water scarcity, adjusting underwriting models and offering incentives for companies that invest in water-efficient practices. By acting now to mitigate these risks, organisations can not only reduce their exposure to water-related disruptions but also contribute to a more sustainable and climate-resilient future.

Inability to attract green skills talent

One of the most important emerging risks in organisations relating to climate change and internal capacity building, is the allocation of adequate resources and sufficient "green" skills and expertise to devoted to managing climate and wider ESG risks. It is important to firstly define Green Skills. The UK Government Post and European Commission define Green Skills as: 'the knowledge, abilities, values, and attitudes needed to live in, develop and support a society which reduces the impact of human activity on the environment'

In respect to green jobs the Green Jobs Taskforce, a UK government advisory body, defines green jobs as those "in an activity that directly contributes to—or indirectly supports—the achievement of the UK's net-zero emissions target and other environmental goals, such as nature restoration and mitigation against climate risks". In respect to the growing demand of green skills and jobs The ONS highlights that green skills span "from energy efficiency and renewable energy installation skills to those needed in the circular economy" emphasising that training programs should focus on both "technical expertise and the management of sustainable practices within various organisational roles"

From a risk management perspective, there is a general view that insufficient resources are being allocated to deal with a wide range of threats and opportunities. This is partly related to the lack of adequate skills and experience.

"Green" capacity building is one of the most important areas of focus for organisations to allocate adequate resources to, the sufficient skills and expertise are required when managing ESG risks related to this.

It is increasingly important to build risk and sustainability teams that have a blend of technical expertise, strategic thinking, and interpersonal skills to manage complex and evolving challenges related to climate risks.

To be a risk manager covering ESG and specifically climate change in 2025 and beyond, there is an evolving range of new skills that are required. Most notably those include lawyer traits, scientific skills, geopolitics knowledge, mathematician tendencies, and resilience.

It is important that risk managers also appreciate their evolving roles and the need to utilise new risk management tools and techniques that require the assessment of ongoing and emerging threats and opportunities.

Organisations must consider partnering with educational institutions and industry peers to develop comprehensive 'green skills training programs' and disseminate best practices and guidelines. By fostering collaboration and investing in workforce development, risk organisations can build resilience against the green skills shortage.

Failure to meet climate emissions targets

The risk of failing to meet climate emissions targets looms large for organisations worldwide. This failure carries significant consequences, including potential fines and penalties imposed by regulatory authorities, as well as the growing threat of climate litigation due to excessive emissions.

Climate litigation is on the rise, with an increasing number of cases targeting governments and corporations for failing to meet Greenhouse Gas (GHG) emissions targets. In 2023 alone, over 230 new climate-related cases were filed globally, demonstrating the urgency of this issue. Cases often focus on the inadequacy of government policies and corporate actions that fall short of international climate commitments and scientific recommendations (Climate Case Chart, 2023).

A key trend within climate litigation is the prevalence of "greenwashing" cases, where companies are accused of misleading consumers about their environmental commitments. Approximately 70% of resolved greenwashing cases result in the jury siding with the plaintiff, reflecting a heightened focus on corporate transparency (Grantham Research Institute, 2023). Additional trends include an increase in ESG backlash cases and landmark rulings from bodies like the European Court of Human Rights, linking climate action to human rights.

Governments face mounting pressure to update their emissions reduction plans and clarify their strategies. Legal victories in one jurisdiction often catalyse similar actions globally, fostering momentum for enhanced climate mitigation efforts (Spain Floods, 2023).

Notably, directors and officers are increasingly targeted in emerging cases for their management of climate risks, highlighting evolving liabilities (Reinsurance News, 2023).

Additionally, the reputational damage resulting from missed targets can severely impact stakeholder trust, customer loyalty, and investment prospects, potentially leading to divestment. From a risk management perspective, risk managers face the challenge of rapidly adapting to evolving business strategies as companies strive to reduce their carbon footprint.

To address this, risk managers must develop comprehensive transition plans aligned with emissions reduction targets set over various time horizons. These plans should integrate robust monitoring systems, allowing organisations to track progress and adjust strategies proactively.

By embedding climate risk management within core business operations, companies can mitigate liabilities, bolster resilience, and seize opportunities in the transition to a low-carbon economy.

Enhanced decarbonising innovations including carbon capture and storage

The landscape of decarbonization is rapidly evolving with innovative technologies emerging to combat climate change. These advancements include renewable energy solutions particularly solar and wind, low-carbon energy sources, electric mobility, and energy-efficient technologies. Among these, carbon capture and storage (CCS) stands out as a critical innovation in reducing carbon emissions.

According to the International Energy Agency (IEA, 2023), CCS could mitigate up to 14% of global CO_2 emissions by 2050 if implemented at scale. Companies investing in CCS not only improve their sustainability credentials but also reduce their risk of non-compliance with emissions targets.

Additionally, governments offering subsidies or tax breaks for CCS adoption present opportunities for organisations to integrate this technology into their climate strategies.

Recent advancements in CCS technology include:

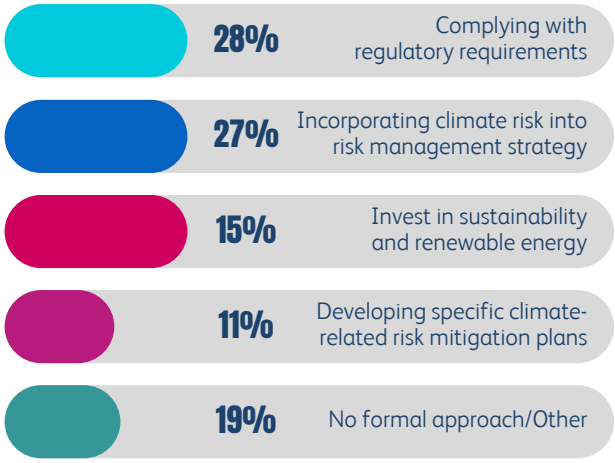
- Material developments unlocking higher carbon capture potential.
- Direct Air Capture (DAC) projects capable of extracting CO_2 directly from the atmosphere.
- Cost-saving innovations that promise more affordable carbon capture methods.
- Biohybrid photocatalysts designed for sustainable and efficient CO_2 capture.
- (Elsevier, 2023) (https://www.elsevier.com/connect/5-key-carbon-capture-technology-trends-for-2023)

From a risk management perspective, these advancements offer opportunities and pose challenges.

Risk managers must remain informed about evolving regulations around CCS and other decarbonization technologies. Additionally, they need to consider global initiatives like the Alliance for Industry Decarbonization, which promotes the adoption of green hydrogen and bioenergy with CCS, as highlighted at COP29 in Baku, Azerbaijan.

The implementation of CCS and similar technologies require substantial investment and specialised expertise, posing financial and operational risks. Therefore, organisations should proactively assess the viability and long-term benefits of these innovations. Through comprehensive risk assessments and strategic planning, risk managers can enable organisations to capitalize on the benefits of CCS and other decarbonization technologies, fostering resilience in the transition to a low-carbon economy.

We asked practitioners what their organisation's primary approach to addressing climate-related risks is?



Climate Transition Risks: Still in the Spotlight for 2025

As economies accelerate their shift toward low-carbon models, financial institutions face heightened transition risks in 2025. Clients in high-emission industries are under increasing pressure from stricter regulations, such as carbon taxes, and shifting market preferences.

Financial institutions are also addressing these challenges. Some have ceased investments in new bonds from oil and gas exploration companies, reflecting a strategic move away from high-carbon industries to mitigate portfolio risks and support sustainability goals. Others have committed to achieving net-zero emissions by 2050, integrating environmental due diligence into credit assessments and setting greenhouse gas reduction targets for key sectors.

Additionally, climate scenario analysis methodologies are being developed to measure the impact of transition risks on portfolios, enabling more informed risk management strategies.

To mitigate transition risks, financial institutions must integrate climate considerations into credit risk assessments, identify vulnerable clients, and adjust lending criteria to favour low-carbon industries. Failure to act could lead to financial instability, reputational damage, and regulatory penalties. These proactive measures not only safeguard financial health but also position institutions as leaders in sustainable finance, ensuring resilience in a rapidly greening economy.

Climate Change Group Update

In 2024 the IRM Climate Change Group committee was restructured with several new members focused with the for us still to on coordinating seminars for the Group members and collaborating with other IRM Special Interest Groups and Regional Interest Groups.

The most recent seminar on green skills and capacity building helped in October explored the development of green skills, covering technical and behavioural aspects and how they align with professional standards.

Having supported the IRM for over 25 years I was truly honoured and grateful to have won and the inaugural IRM Risk Management Leader of the Year Award at the CIR award in London in November that was presented to me by the IRM Chair Stephen Sidebottom. In order to continue to support risk professionals in 2025 the Committee has agreed to restart the “Climate Change Matters” Newsletter to help provide greater insights into government and regulatory climate updates as well as provide sections of risk management best practices and details of relevant events and conferences.

IRM Ambassador Insights

Paul Saunders

Chair of IRM's Operational Risk Group, supported by the following contributors from Projective Group, Toby Pearson, Jon Szehofner, John Parker, Will Thomas, Osama Khan, Helen Weaver and Sonny Davies

Written by:
Paul Saunders
Managing Director GDFM Consulting, Part of Projective Group

Introduction

2024 has again been a challenging year for Operational Risk Manager, with ongoing changes in the operational environment, coupled with new regulations, driving the continued need for organisations to adapt. This means they must continue to evolve their governance, people, processes, and systems for internal control. Here we look at some of the trends that we believe will continue to pose challenges for organisations in 2025.

Geopolitical Risk

The traditional pillars of peace and prosperity can no longer be taken for granted. A confluence of economic trends and geopolitical upheavals - including conflicts in Europe and the Middle East, inflationary pressures on consumers and businesses, banking sector instability, global recession fears, pandemic aftershocks, labour market disruptions, and fierce competition for digital talent - is all contributing to reshaping the global order.

Amid these shifts, globalisation itself is being redefined. National security priorities and assertive policy interventions, especially among the world's major powers, are reshaping global trade, supply chains, and economic integration. In this new reality, geopolitical developments are set to further disrupt supply chain strategies, redirect investment flows, and increase operational costs for businesses.

Once celebrated for their complexity and efficiency, integrated global supply chains are now seen as vulnerabilities, prompting companies to rethink their strategies in the face of intensifying geopolitical competition.

This has fuelled a growing emphasis on national industrial policies that favour domestic suppliers and promote 'onshoring' or 'friend-shoring' in critical industries such as semiconductors, energy, pharmaceuticals, and defence.

While this approach is designed to enhance resilience, it also entrenches inflationary pressures, making them more persistent than previously anticipated.

Resilience

The two regulations driving resilience - such as DORA (Digital Operational Resilience Act) and the UK PRA regulations - are shaping the direction of risk management practices in the financial sector.

These regulations emphasize the need to assess and report on operational risks, a critical requirement for stability and longevity. Although there are differences in scope between DORA and the UK PRA (with DORA being more prescriptive and the UK PRA more self-defining), they have driven standardised, consistent operational models, particularly for organisations with a European footprint.

For instance, both IT and non-IT incident management, as outlined by DORA and the UK PRA respectively, need to be similarly rigorous and robust across all European locations. The 2024 CrowdStrike incident has further highlighted the importance of identifying critical third parties and understanding the risk profile of each. Third-party registers, tighter contracts, and the identification of additional vendors have enhanced transparency and bolstered resilience.

Complying with these regulations is just the beginning. The spirit and intention of resilience regulation is beginning to take hold, and regular testing will identify weaknesses in controls and result in continuous improvement.

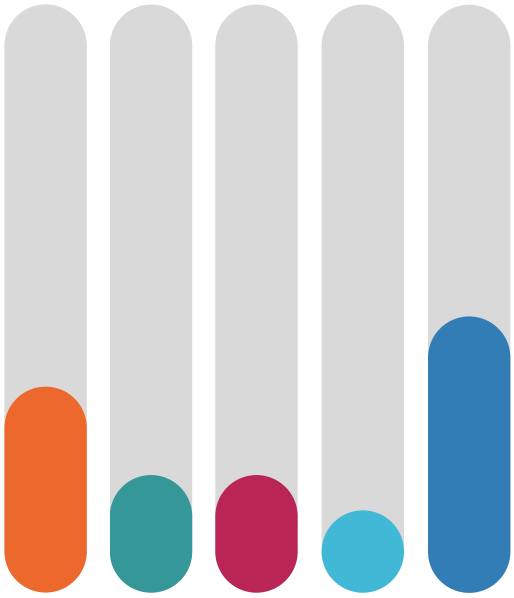
Financial Crime

Financial crime has surged to its highest levels in years, a trend often exacerbated during periods of economic strain. This increase has been amplified by the rapid shift toward digitalisation, exposing societal naivety about how these evolving systems function. Reports of fraud continue to grow, with law enforcement agencies cautioning that reported cases likely represent only a small fraction of the actual incidents.

Consequently, the volume of illicit proceeds requiring laundering has grown significantly, placing heightened pressure on anti-money laundering (AML) systems and controls within regulated sectors.

This challenge is further compounded by new regulatory frameworks, such as the Payment Services Regulator's (PSR) APP Scam Reimbursement Rules, which impose stricter obligations on banks and payment service providers.

What do you believe will be the greatest challenge for risk management professionals in 2025?



30% Keeping up with rapidly changing technology and cyber threats

11% Managing the growing complexity of global regulations

10% Addressing climate-related risks and sustainability

4% Ensuring workforce diversity and talent development

45% Balancing cost efficiency with comprehensive risk coverage

These rules demand robust fraud detection and prevention systems to meet stringent reimbursement deadlines and shared liability requirements. Strengthening operational frameworks is essential not only to meet compliance mandates but also to ensure resilience in an environment of escalating financial crime. By embedding a forward-looking approach that includes horizon scanning and strategic planning, organisations can better position themselves to mitigate risks, safeguard their operations, and maintain operational resilience in the face of increasing regulatory and financial crime pressures.

ESG

Over the past year, sustainability-related work has increased significantly, driven largely by the EU Corporate Sustainability Reporting Directive (CSRD). Under this directive, the largest public companies are required to submit their first CSRD reports by 2025, with a second wave of large companies following in 2026. In the UK, the government plans to introduce new sustainability reporting standards by the first quarter of 2025. These will align with the IFRS Sustainability Disclosure Standards (SDS) and integrate with the UK's broader Sustainability Disclosure Requirements (SDR). Adoption is targeted for July 2025, reflecting a commitment to aligning with international frameworks. One key area of focus is the accurate reporting of greenhouse gas (GHG) emissions.

Companies increasingly need to look beyond their own operations and engage with their value chains - particularly suppliers - to gather reliable emissions data. As a result, procurement teams face growing demands for third-party reporting, adding complexity to an already considerable compliance effort. However, this work is crucial for setting credible net-zero targets and implementing effective transition plans. Given these heightened requirements for disclosure and reporting, it is essential for companies to take control of their sustainability data. Leveraging appropriate tools and technologies can help streamline processes and manage these challenges efficiently.

Cybersecurity

As cyber threats become increasingly sophisticated, financial institutions must prioritize cyber resilience to protect their operations and customer data. The rising supply chain risks, exacerbated by the globalisation of business operations, have made it easier for threat actors to exploit vulnerabilities within interconnected systems.

Moreover, the increased use of AI for cyber attacks - including social engineering and deepfakes - has introduced new challenges. These AI-driven threats, combined with intensifying geopolitical tensions, have led to increased activities from both state and non-state actors.

The low barriers to entry for cybercriminals, coupled with the increasing sophistication of ransomware attacks, have heightened the urgency for robust cyber resilience strategies. Effective cyber resilience not only involves preventing and responding to cyber incidents but also ensuring the continuity of operations and the ability to recover swiftly from disruptions. Regulatory frameworks such as DORA in the EU and the UK Operational Resilience Act underscore the importance of maintaining high standards of cyber resilience. These regulations mandate that financial institutions implement comprehensive measures to protect against, respond to, and recover from cyber threats.

Risk Control

Risk control working practices are growing in maturity and this is coupled with increased expectation from regulators in the level to which they are embedded in the working practices. Risk and Control Self Assessment (RCSA) is a minimum expectation and is now a key part of day-to-day management of operations and change delivery. This can add significant complexity and cost both due to the need to support data driven and automated operational risk monitoring.

The complexity and variety of threats faced across all markets is pushing organisations to ensure roles and responsibilities between different departments - such as operations, technology, finance, and legal - are unambiguous and result in a holistic approach to risk management. A trend of creating and testing playbooks to test scenarios is emerging. While this can be costly in terms of time investment, it can save vital hours in the management of real-life scenarios.

Conclusion

Whilst the six themes listed above are in no way the only things organisations have to consider, they do represent those that should be high up on an organisations risk agenda and be monitored closely by Business Leaders, Risk Committees and Boards.

IRM South East Asia Lead Insights

Written by:
Annie Tay
Managing Director GDFM Consulting, Part of Projective Group

Annie Tay has served as Chief Risk and Compliance Officer for multinational financial institutions and fintechs. Annie's experience is in enterprise wide risk management spanning strategic, financial, operational and business risks, in particular in insurance, pensions, investment and finance. Her focus areas encompass innovation in the morbidity and longevity risks, financial market volatilities, and man-made and natural catastrophic risk management, with the overarching goal of supporting the knowledge to underpin a sustainable ecosystem for all.

Staying Ahead of the Curve: Key Trends in Asia

Risk management in Asia is influenced by a myriad of factors, as a region with diverse economies and political and regulatory landscapes, Asia presents unique challenges for risk professionals and businesses operating in the region.

Top Three Risks to Watch in Asia 2025

The latest World Economic Forum (WEF) report highlights several top risks that are particularly relevant to Asia:

- State-Based Armed Conflict: This remains the most pressing immediate global risk for 2025, reflecting heightened geopolitical tensions and fragmentation globally.
- Extreme Weather Events: Environmental risks dominate the longer-term outlook, with extreme weather events being a key concern. Asia is particularly vulnerable to these events, which can disrupt business operations and supply chains.
- Misinformation and Disinformation: These remain top short-term risks, underlining their persistent threat to societal cohesion and governance by eroding trust and exacerbating divisions within and between nations.

Risk managers in Asia face a complex and dynamic environment. By staying informed about geopolitical developments, economic trends, and technological advancements, they can better anticipate and mitigate risks. It is crucial for businesses to adopt a proactive approach to risk management and build resilience against emerging threats.

The IRM is actively expanding its footprint in Asia with a dedicated focus on upskilling and supporting the risk management profession to help businesses remain resilient in a volatile, uncertain, complex, and ambiguous (VUCA) world.

Through comprehensive education, training, and advisory services, the IRM aims to equip risk professionals with the necessary tools and knowledge to navigate the region's unique challenges.

Key Factors Influencing Risk Management in Asia:

Geopolitical Tensions

The ongoing South China Sea dispute has led to tensions between China and several Southeast Asian nations, impacting maritime trade routes and security.

Trend: Confrontation

The continuing trade tensions between major economies, particularly the US and China, are likely to persist. This can lead to increased tariffs, trade barriers, and economic uncertainty, necessitating contingency plans and diversified supply chains for businesses.

Economic Volatility

The rapid economic growth in India has spurred infrastructure development but also resulted in challenges such as urban congestion and inflationary pressures.

Trend: Market Fluctuations

The varying stages of economic development across Asia lead to differing levels of economic stability. Businesses must remain agile, utilising diversification and scenario planning to navigate periods of rapid growth and downturns.

Regulatory Changes

China's recent data privacy law (PIPL) has significant implications for companies handling personal data, requiring stringent compliance measures.

Trend: Regulatory Compliance

With the introduction of new regulations, companies will need to stay compliant with evolving standards, including data protection laws, environmental regulations, and corporate governance requirements. Adopting robust compliance frameworks will be critical.

Technological Risks

The WannaCry ransomware attack affected several Asian countries, causing significant disruptions to businesses and healthcare systems.

Trend: Cybersecurity Threats

Malaysia's Role as ASEAN Chair for 2025

In 2025, Malaysia has assumed the chairmanship of ASEAN, marking its fifth time leading the regional bloc since its establishment in 1967.

Under the theme of "Inclusivity and Sustainability," Malaysia aims to strengthen regional cooperation, enhance economic integration, and promote sustainable development.

This leadership role presents significant opportunities for businesses in the region, as Malaysia will host over 300 key meetings and programs throughout the year, focusing on areas such as artificial intelligence, renewable energy, tourism, and healthcare.

By fostering collaboration and driving initiatives that align with ASEAN's goals, Malaysia's chairmanship will contribute to a more resilient and prosperous regional business environment.

Environmental Risks:

Typhoon Yagi (2024): This powerful storm caused severe flooding and landslides across Southeast Asia, including Vietnam, Laos, Thailand, and Myanmar. The death toll surpassed 250 people, with millions struggling with flooded homes and power cuts.

Malaysia and Southern Thailand Floods (2024): Heavy monsoon rains led to widespread flooding in Malaysia and southern Thailand, displacing tens of thousands of people and resulting in over 30 fatalities.

Mount Ibu, Indonesia (2025): This remote volcano on Halmahera Island has erupted over 1,000 times since January 1, 2025, with ash plumes reaching up to 4 kilometres high. Authorities have evacuated around 517 residents so far, but many remain due to ongoing crop harvests.

Trend: Climate Change Impact

The impact of climate change and environmental degradation is becoming more evident, with extreme weather events becoming more frequent and severe. Businesses will need to incorporate climate risk and ESG considerations into their strategic planning and operations to build resilience.

Misinformation and Disinformation:

During the 2024 Indonesian Presidential Election, there was a significant spread of misinformation and disinformation through social media platforms. False claims about candidates, manipulated videos (deepfakes), and misleading information about election processes created confusion among voters and undermined trust in the electoral system.

This disinformation campaign highlighted the growing challenge of combating false information in the digital age and its potential to destabilise democratic processes in Southeast Asia. The impact was felt across the region, as neighbouring countries observed the effects of misinformation on public trust and governance.

Trend: Societal Risks

The persistent threat of misinformation and disinformation can erode trust and exacerbate divisions within and between nations. Risk professionals must develop strategies to counter these threats and promote accurate information.

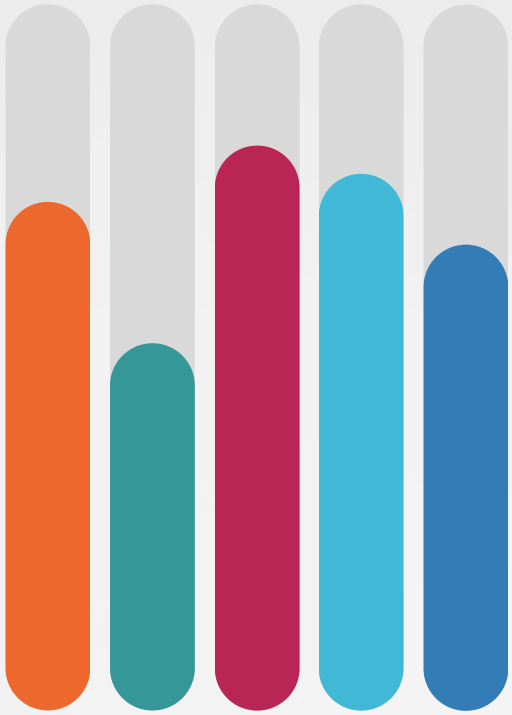
Insights from Risk Professionals in Asia

Recognising these regions' diverse and untapped potential, the IRM is dedicated to establishing a strong foothold in Asia through corporate partnerships, targeted academic collaborations, events with regulators, members and local businesses.

72% identified technology and digital risks as requiring the biggest investment or change

52% believe AI will have the greatest impact on risk management practices in 2025

80% believe the demand for qualified risk experts will increase over the coming year

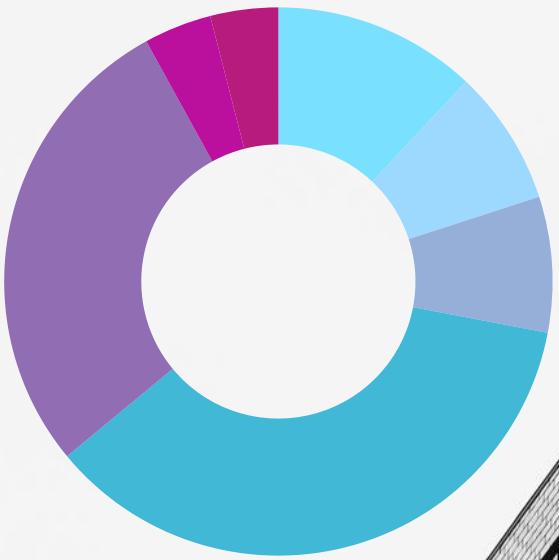


76% indicated that it is difficult to recruit qualified risk professionals in Asia

32% indicated that they were not confident in their ability to identify and assess future risks with their current resources (specifically the tools and technologies available at their disposal)

We asked what was your organisation's biggest challenge in managing risks effectively in 2024?

- **36%** Integrating risk management across departments/functions
- **28%** Lack of skilled personnel
- **12%** Insufficient budget and/or resources
- **8%** Regulatory complexity and/or compliance burdens
- **8%** Difficulty in identifying and assessing emerging risks
- **4%** Slow adoption of new technologies
- **4%** Other



08 Australia Regional Group

Written by:
Colin McCrorey
Managing Director,
Victorem

Colin McCrorey

Colin McCrorey (SIRM) is the founding Chair of the Australia regional group and an approved provider of the IRM Fundamentals of Risk Management (FoRM) course. He is the current Managing Director of VICTOREM, a specialist Risk Management and SESA specialist consultancy located in Sydney. Colin has over 20 years of experience in Risk Management across numerous countries and on some of the largest projects and organisations globally. Colin specialises in major infrastructure project risk management across numerous sectors including transportation, energy and defence.

Additional Contributors:

- Anh Dinh
- Rynier Brandt
- Carl Fernando
- Jason Rohloff
- Michael Porteous

With the population of Australia continuing to rapidly grow, we're certainly not slowing down anytime soon. We predict 2025 to be another year of change and continued evolution for our great nation. With growth comes demand. Demand for greater infrastructure, technology, critical resources such as energy, food and water and our security, all of which, puts more pressure on our fragile environment. Looking forward over the next 12 months, Australia's focus should be directed at these key threats.

Geopolitical risks

Australia's geopolitical risk rating is relatively low when compared to the rest of the world. The return of a Trump presidency presents significant geopolitical risks for Australia and the Indo-Pacific region, particularly regarding security alliances, trade relations and Trump's isolationism through trade-tariffs. Any disruption to regional dynamics can have a direct and indirect (contagion) impact on Australia and its close neighbours. At a time when relations between China and Australia have been easing, deepening ties with the US through initiatives like AUKUS now also present complexity as US-China tensions continue to rise. This tension has led to trade disputes, cyber-attacks, and diplomatic conflicts, impacting Australia's economic stability and international standing. China is Australia's largest export partner by far, with $218bil in exports representing 32.6% of total exports in 2023. To put this in perspective, Japan, which is Australia's second largest export market made up only 13.4% and the other export partners in the top five in single digits.

Additionally, the threat of cyber-attacks and espionage from countries like China and Russia is increasing, compromising sensitive information and critical infrastructure. Australia also has concerns and will direct focus towards China's increasing influence on Pacific Islands, which continue to pose significant challenges. Australia's interconnectedness within regional trade networks and financial systems makes it more susceptible to deglobalisation pressures. This exposure is highlighted by a 2024 political risk survey indicating 70% of international firms reported political-risk related losses. This underscores the imperative for government and business leaders to strengthen regional resilience and agency whilst balancing strategic outcomes. Recent anti-Semitic incidents spilling over into Australia from the conflict in Gaza has caused concerns about the long impact on social cohesion and the need for Australians to maintain its status as a safe haven for all its citizens, especially minority groups.

Technological risks

Australia's AI landscape presents both transformative opportunities and significant risks. While Microsoft projects annual revenues of A$18.8 billion from data and data centre capabilities alone, and the Tech Council forecasts generative AI could contribute A$115 billion annually to the Australian economy by 2030, public concern remains high.

A University of Queensland survey reveals 80% of Australians believe AI risk should receive the same priority as pandemic and nuclear threat preparation. The nation's extensive digital infrastructure amplifies AI-related vulnerabilities, particularly regarding misinformation and data integrity, data quality and governance. The nation's extensive digital infrastructure amplifies AI-related vulnerabilities, particularly regarding misinformation and data integrity. Data quality and governance emerge as fundamental pillars of risk management in this AI-driven environment. Socioeconomic challenges loom large, from workforce automation to widening inequality and urban-rural digital disparities. CSIRO research emphasizes that beyond mere access, AI literacy and capability development are crucial for inclusive adoption and risk mitigation. The regulatory landscape is evolving in response to legal and ethical concerns around privacy, consent, and transparency. While the government has introduced voluntary safety guardrails, organisations face increasing compliance risks when adopting AI without robust governance structures.

Clear mandatory requirements for AI implementation will be essential to boost business confidence while managing potential exposures. Cybersecurity continues to be of concern, exacerbated by international actors and commercial interests in major defence projects such as the AUKUS. This is a trend that spans across all industries and includes significant risks like loss of personal identifiable information, infrastructure damage, financial losses through ransomware and intellectual property losses. Cybersecurity has been a key priority for Australia's prudential regulator the Australian Prudential Regulation Authority (APRA). APRA reconfirmed its commitment to maintain its heightened focus on cyber resilience, this comes on the back of the growing threat of cyber-attacks faced. The previous CEO of National Australia Bank revealed the banking sector were experiencing an estimated 50 million attacks per month. The need for capable people to address the ever-changing technological environment is a risk that requires State and Federal support and strategies across all industries.

Environmental / Climate risks and Environmental Pressures

It's no secret that Australia has its fair share of the impacts due to the effects of climate change, whether that be bushfire, flooding or other. With biodiversity being quoted by many including the UN as the best defence against climate change, Australia must focus on conserving, restoring and removing the harmful elements such as carbon dioxide from our atmosphere. With 2024 being one of the warmest years on record, Australia's weather and climate has seen hotter days, drier land, longer fire seasons, decreasing rainfall and rises in sea level. To help the country in staying abreast and preparing for this challenge, Australia's first scientific evidence based National Climate Risk Assessment has been conducted. From legislative perspective, climate-related financial disclosures will apply to certain Australian companies commencing 1 January 2025. While Australia has made commitments to combat climate change, many of these actions are long term, including committing to achieving net-zero emissions by 2050. For this, there is much criticism and a need for short term climate change wins. It is essential from the outset to remind all of us to look both sides of the coin, the downside and upside of environmental / climate risks. Failure to consider climate risks in strategy planning will do the organisation a disservice in the long run. Public's expectations on organisations' demonstration of concrete commitment towards environment sustainability should be considered.

The impacts of climate risks have already been observed in the insurance sector including higher excess and exclusions (such as flood cover), and supply chain disruptions, transferring the risk on the everyday Australian with regards to protection of their assets. Premiums continue to rise, and it is expected they follow suit of previous years to be well above the annual CPI increase. With the geopolitical pressures in the region and our increasingly closer relationship with the US, any policy changes implemented by the Trump administration, who withdrew from the Paris Agreement when last in office, may add pressure to Australia to follow in similar footsteps. There will need to be a good balance between maintaining strong relationships and maintaining commitments towards a better environment for our future generation. While Australia has plenty of environmental threats to be concerned about, there is an upside. The nation has seen significant investment and growth in the renewable sector with solar and wind power leading the way. Hydrogen economy is currently being explored. Additionally, the country has seen large increases in electric vehicles, a trend that is set to continue into 2025 and beyond. The Australian Financial Industry has a significant role to play to support the funding of renewable projects and can have a significant impact on the speed of addressing climate change.

09

East Africa Regional Interest Group

Written by:
Sospeter Thiga
Co-Chair,
East Africa Group

Sospeter Thiga

Sospeter Thiga is a seasoned ESG expert and leader in Enterprise Risk Management with over 18 years of experience across industries such as financial services, renewable energy, and real estate. As the Group Head of Risk & Quality Assurance at CPF Financial Services, he leads critical initiatives in risk management, business continuity, and compliance. Sospeter has driven key projects such as automating performance systems, launching an ethics program, and developing a robust compliance framework. He works closely with the CEO on public policy and regulatory reforms, and actively contributes as a board member for organisations like Tanari Trust and Utana Foundation.

Written by:
Catherine Nyaga-Mbithi
Co-Chair,
East Africa Group

Catherine Nyaga-Mbithi

Catherine is a dynamic professional in Governance, Risk Management, Compliance, and Audit, with experience supporting over 50 organisations across Africa and Europe. As an Internal Audit Manager at Absa Group, she oversees audits, develops risk-based plans, ensures compliance, and advises senior leadership. Her expertise includes board leadership, governance reviews, and capacity building, all aimed at optimising performance and strengthening controls. A member of the Audit and Risk Committee of the Institute of Risk Management, Global, Catherine is a trusted partner for organisations navigating complexity and driving sustainable success.

Additional Contributors

Sheila Mueni Mulinge
Office Manager
Institute of Risk Management Africa

> These risks are not only driven by internal vulnerabilities but also influenced by global geopolitical and climate-related shifts.

Introduction

In 2025, East Africa will face an evolving risk landscape shaped by political, economic, societal, environmental, and cybersecurity challenges. These risks are not only driven by internal vulnerabilities but also influenced by global geopolitical and climate-related shifts. Below is a detailed projection of the most pressing risks, supported by analysis of their potential drivers and impacts.

1. Economic Risks: Debt Sustainability and Financial Liquidity

Persistent economic challenges stem from high public debt and inflation. Kenya's heavy debt repayments, combined with inflationary taxation under the Finance Act, constrained fiscal space, while Ethiopia's post-conflict recovery slowed economic rebound. Reduced access to concessional loans and tighter global monetary conditions may exacerbate fiscal strain. Fragile financial liquidity in Kenya and Ethiopia could drive credit downgrades, undermining investor confidence. Effective restructuring and prudent fiscal reforms will be critical to stabilise economies.

2. Political Risks

In June 2024, widespread protests in Kenya arose in response to the Finance Act, which introduced higher taxes on fuel and essential goods. On June 25, demonstrators entered Parliament, leading to confrontations with law enforcement amid allegations of excessive force. The demonstrations reflected public concerns over rising costs of living, economic inequalities, and governance challenges. The unrest highlighted underlying societal grievances and eroded public trust in governance structures. As 2025 progresses, unresolved economic challenges and governance issues may contribute to further public dissent if conditions do not improve.

Ethiopia continues to face governance challenges due to ethnic conflicts in Amhara and Oromia, despite peace agreements with Tigrayan forces. Somalia has made progress against al-Shabaab militants, yet clan tensions and reduced African Union peacekeeping support present ongoing governance hurdles. Meanwhile, Sudan's civil war has spilled over into neighboring countries, disrupting trade and worsening humanitarian crises. In addition, South Sudan faces continued instability driven by inter-communal violence, localised armed group conflicts, and the spillover effects of the Sudan crisis. These challenges will likely affect regional stability and economic cooperation across East Africa in 2025.

3. Regulatory challenges

In 2025, continued reliance on tax reforms to address fiscal deficits poses risks of further public backlash and reduced investor confidence. Regulatory unpredictability, especially sudden tax increases or enforcement measures, will remain a challenge for businesses seeking stability in economic environment of countries like Kenya.

63% of practitioners in Africa identified stability in the economic environment as an emerging risk in 2025.

4. Environmental and Climate Risks

East Africa's vulnerability to extreme weather events remains a significant concern, with floods and drought cycles expected to intensify in 2025. In 2024, the El Niño weather phenomenon caused unprecedented rainfall during the March-May rainy season.

In Kenya, torrential rains resulted in displacement as well as economic and societal disruption across the region, including in Somalia, Tanzania, and Burundi. Major flooding occurred in Tana River County and Baringo in Kenya, leading to the destruction of homes, schools, and farms.

Floods also disrupted access to clean water, increasing the risk of cholera outbreaks in densely populated areas. Alternating cycles of drought have worsened in arid regions, particularly Turkana and Garissa in Kenya and southern Somalia, leaving millions of people food-insecure.

The reliance on rain-fed agriculture remains a critical weakness, as climate variability disrupts harvests. In 2025, these weather extremes will likely escalate humanitarian needs and force climate-induced migration

5. Societal Risks

In 2024, femicide and gender-based violence (GBV) surged across East Africa, particularly in Kenya. Civil society groups reported an increase in intimate partner violence and femicide cases, driven by economic stress and societal inequalities.

These risks are expected to persist in 2025 unless more robust protective measures and legal frameworks are implemented.

Youth unemployment remains a persistent issue in East Africa. The lack of formal job opportunities, coupled with rapid urban migration, has strained cities' infrastructure and increased reliance on informal work. By 2025, this trend is expected to deepen, risking further disenfranchisement of the youth population and fueling potential unrest. Governments need to invest in education, vocational training, and job creation to address this systemic challenge.

6. Cybersecurity Risks: Emerging Digital Vulnerabilities

East Africa's growing reliance on digital systems exposes it to heightened cybersecurity risks. In 2024, phishing and ransomware attacks targeted Kenya's fintech ecosystem and Uganda's banking sector. Cybercriminals increasingly used AI to craft sophisticated scams, exploiting weaknesses in government and private sector IT systems. The risk of data breaches and financial fraud will grow as digital transformation accelerates. Investments in cybersecurity infrastructure and regulatory enforcement will be crucial to mitigate these threats.

13% of practitioners in Africa highlighted that AI helped them improve their daily activities at work

54% of practitioners in Africa believe their orgnasiation is somewhat prepared to manage risks associated AI.

7. Geopolitical and Resource Risks

The growing global demand for critical minerals such as lithium and cobalt intensify competition in East Africa. While a country like Tanzania attracts foreign investments into their mining and energy sectors, the "resource nationalism" trend is raising risks. Governments are revising mining codes to demand higher stakes for state enterprises, increasing regulatory challenges for foreign companies.

For example, Tanzania may ban the export of unprocessed critical minerals to support its domestic economy but risks discouraging investors. Balancing national interests with foreign partnerships will be crucial for resource-rich nations like Tanzania to maximize economic benefits while avoiding overregulation.

Conclusion

East Africa's risk outlook for 2025 highlights the importance of proactive strategies to address systemic vulnerabilities and seize emerging opportunities.

The lessons of 2024, including the economic pressures, climate crises, and governance gaps, underscore the need for long-term resilience planning.

Decision-makers must act decisively to mitigate risks while leveraging growth opportunities in technology, infrastructure, and resource management.

By prioritising these measures, East Africa can build resilience, stabilise economies, and create sustainable growth pathways for 2025 and beyond.

Recommendations for Decision-Makers:

1. Align Risks with Strategy: Integrate identified risks into strategic and business planning to enhance organisational resilience.
2. Scenario Planning: Utilise scenario-based risk assessments to prepare for different potential outcomes and impacts.
3. Adapt Key Performance Indicators (KPIs) to Evolving Risks: Develop flexible performance indicators to adjust strategies based on dynamic risk landscapes.
4. Inform Stakeholder Decisions: Use comprehensive risk data to support informed decision-making across public and private sectors.

10 India Regional Interest Group

Written by:
Rajeev Tanna
Head – Risk Management, Strategy and Internal Compliance, Tata Consulting Engineers Ltd.

Rajeev Tanna

Rajeev has over 30 years of experience in the fields of Risk Management, Consulting and Financial Services with organisations like Tata Consulting Engineers, Cairn Oil & Gas Division - Vedanta Limited, GMR Infrastructure, Deloitte, Aon and IndusInd Bank. He has been heading the Enterprise Risk Management (ERM) Function for a large Conglomerate for over 15 years and has over 6 years of ERM consulting experience. His education qualifications include BE (Electronics), PGDBA (Finance), CFIRM, ACII, FIII, CAIIB and DRMC (IRM).

JOIN

Bold Ambitions

India has bold ambitions of being a developed nation by 2047 and continues to be the fastest growing economy in the world despite all odds, especially after the pandemic.

The trend has been projected to continue likewise in short to medium term as projected by the International Monetary Fund (IMF). India has been on a growth trajectory in recent times.

The significant milestones include substantial improvement in food security, widespread economic reforms, enhanced per capita income, improvement in number of people above the poverty line, and becoming a global software hub.

"With the ever-increasing rush to adopt emerging new technologies and advancements to gain competitive advantage in a volatile and fast-moving risk landscape, a robust focus on risk management will be key to overall success of the country as well as organisations as we are operating in a "CUVVI world". CUVVI stands for Complex, Unpredictable, Vague, Volatile, and Interlinked."

Though projected for long term growth, the economic growth dwindled compared to expectations and moderated to 5.4% in the Q2 of FY '25, down from 8.1% in the same period last year and 6.7% in the Q1 FY 25. This slowdown, attributing it to weaker consumption, subdued government spending, and adverse weather impacts on key industries

Technology Risks:

Cyber Attacks/Data Breaches: With the increase in digitisation trend, risks of its misuse have also increased especially in India. As per an online report, India faced nearly 370 million malware attacks in 2024, with ransomware detections exceeding one million. Banking, Financial Services & Insurance (BFSI), Healthcare, Hospitality, E-Commerce, etc. were top targets. Cyber incidents are one important aspects to watch out for in India during 2025.

Integrating existing processes with AI and related technologies could be on cards for most of the organisations in India in near to mid-term.

India's Government has held off on AI-specific regulation, on the premise of existing laws around areas of data protection, fraud and deepfakes. Instead, the Govt is developing a voluntary code on training, deployment, commercial sale and rectification of misuse of LLMs and AI platforms. Meanwhile, Ministry of Electronics and Information Technology (MeitY) is looking to develop legal frameworks to mandate companies developing LLMs to train them on local languages.

It seems to be pointing towards self-regulation regime.

Global aspects Impacting India:

Global Tariffs and Global Trade: The US imposing tariffs on major countries, along with potential return tariffs, is reshaping global trade dynamics. This situation presents both opportunities and threats, especially for India. Trump has warned the BRICS countries he would require a commitment that they wouldn't create a new currency as an alternative to using the USD and has threatened to levy a 100% tariff if they did.

This could lead to uncertainty leading to tariff changes by both US and India impacting the trade between the nations. It will be important to see how India balances out its relations with the West and Russia. As of now, it has kept a neutral stance.

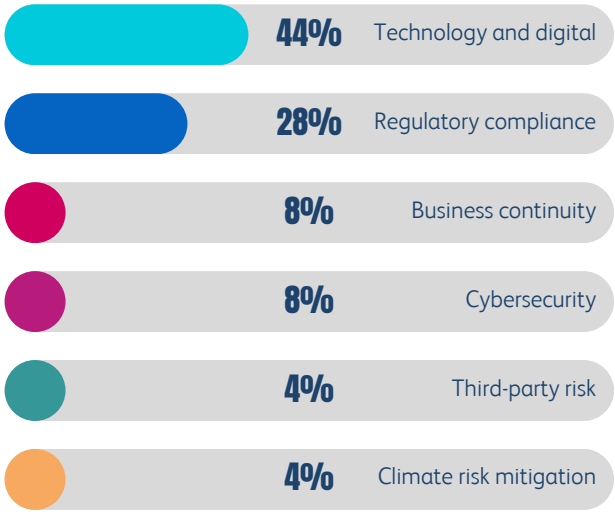
Geopolitical Challenges:

Global conflicts have led to impact on so many aspects especially the oil prices which has the biggest influence on India's Balance of Payments (BoP). Conflict in Middle Eastand Russia-Ukraine conflict influences oil prices.

For India, the softening of global oil prices offers fiscal relief, though geopolitical tensions pose a risk. Heightened geopolitical tensions, especially in the Asia-Pacific region, could disrupt trade routes and increase commodity prices, impacting India's trade balance and inflation. India's neighborhood in chaos: Bangladesh grapples with political instability and protests, Pakistan is in an economic and security crisis, Myanmar is embroiled in conflict post-2021 coup, and Sri Lanka continues to recover from its 2022 economic collapse.

Relationship with China– In 2024, after a long military standoff of 4 years with China, both the countries announced success in disengagement agreement. It will be crucial to observe that both countries are following the agreement conditions as it leads to increased disruptions in trade and China is one of the major trade partners for India. Increased spending on defense also impacts other crucial industries like Infrastructure.

We asked practitioners in India which aspect of risk management has required the most significant investment in 2024?



Economic Challenges

GDP growth – Sustained GDP growth above 7% could be challenging considering the external and internal risks. RBI has slashed GDP Growth Forecast for FY25 From 7.2% To 6.6%. The GDP growth forecast for Q3 FY25 has been revised to 6.8% from 7.4%, while the Q4 projection was lowered to 7.2% from 7.4%, the Q1 FY26 estimate has been adjusted to 6.9% from 7.3%.

Fiscal Consolidation - The government aims to push the fiscal deficit below 4.5% of gross domestic product (GDP) in the next financial year from the budgeted 4.9% of GDP in FY25. The government's efforts to reduce the fiscal deficit could constrain public spending, potentially slowing down economic growth. For a second straight year through FY25, actual government capex is likely to fall short of the target by more than Rs 50,000 crore. This is partly due to the inability of states to fully utilize the Rs 1.5 lakh crore long-term interest-free loans pledged by the Centre to bolster their capex in FY25. In the last fiscal year, capex had hit 95% of the initial allocation of Rs 10 lakh crore.

Inflation - Considering higher inflation, interest rate cuts are not anticipated near term. Inflation remains a significant concern for the RBI. Depending on inflation figures, rate cuts may be announced in 2025 to bolster GDP growth. In October 2024, inflation rose to 6.2%, the fastest pace in over a year, mainly driven by food prices. Inflation levels are still above the RBI's target window of 4-6%. As of December 2024, RBI has kept Repo Rate constant at 6.5% for 11 times in a row.

Reduced global demand - Potential of reduced demand from globe due to conflicts may lead to impact not only on exports of India but also reduced foreign investments like FDI.

Slowdown in Manufacturing - The bulk of the slowdown in Q2 FY25 GDP growth has been due to manufacturing. Role of manufacturing in overall growth is crucial and it will be a key monitorable.

Private Capex - Private Capex is key for growth, and it has remained constant during FY24 over FY23. As per a Care Ratings report, the top 5 sectors in which private capex remain concentrated are Oil and petrochemicals (21% share in total), Power (12.8%), Telecom (12.8%), Automobile and ancillaries (7.4%), and Iron and steel (7.1%) in FY24. It would be crucial for all sectors to participate in private capex for a sustained growth over medium to long term.

Despite these risks, India's large domestic market, stable government, diversified economy, structural reforms, adequate foreign exchange reserves etc. provide significant resilience and cushion against these shocks

Continuation of schemes by government: Government of India has launched various schemes like PLI, Make in India, Scheme for Promotion of Manufacturing of Electronic Components and Semiconductors (SPECS), National Infrastructure Pipeline etc. It will be important to observe how all the aspects related to these schemes are properly addressed.

Availability of Credit: As per an online report, Incremental bank credit growth is expected to slow down to 12% YoY in FY25 compared 16.3% in FY24. It has potential of impacting the overall capex plan that may lead to reduced growth.

Attraction and retention of talent: Demand for high skilled workers leading to tough competition, employee expectations, diversity & inclusion, gaps in skillsets etc. are some of few challenges to name a few.

Climate Change: India is grappling with significant climate risks, including rising temperatures, water scarcity, and frequent extreme weather events. The year set climate records, highlighting the growing impact of climate change, with events like heatwaves, floods, and storms affecting vulnerable populations, as seen in incidents like the unexpected landslide in Wayanad, Kerala.

Pollution: Air pollution remains one of India's most pressing environmental issues. High levels of particulate matter (PM2.5 and PM10) and other pollutants like NOx and SO2 are expected to persist, particularly in urban areas. Regulatory and policy changes risk – Changes in regulations / laws, imposition of new taxes like amendments in corporate tax, Long Term Capital Gain (LTCG) etc. may lead to impact on FPI flows in India or the corporate earnings leading to impact on Capex.

Actionable recommendations and potential strategies which could be considered by Corporates:

Monitoring of risks - Business Intelligence (BI) plays a vital role in helping companies track global aspects and incorporate learnings into their business strategies. Some of the aspects that are crucial from BI perspective are shared as below:

BI helps enabling availability of data from global sources with diverse views of multiple aspects like Geopolitics, evolving risks in the geographies, competitive landscape, standard metrics etc. which helps in adjusting the strategies and understanding the risk associated with the business of respective organisations.

Development of inhouse tools or taking subscription of digital tools that may provide such data may prove to be very helpful in taking risk adjusted calls.

It also helps in real time analytics and predictive analytics enabling swift responses to changes and opportunities. Dashboards and Reporting: Dynamically changing dashboards with access-based controls as per the company requirements may help in ensuring all KPIs are being tracked and reported to senior management to ensure timely action.

Mitigation of Adaptation of risks:

Contingency funds or Contingency Reserves to deal with unexpected or unpredictable situations or emergencies. This aspect has gained even more prominence post Covid-19.

Stress testing the portfolio of assets and liabilities at regular intervals. It is important to periodically conduct vulnerability assessments to check what are the key risks and their impacts that organisation is most exposed to, for planning suitable mitigation strategies.

Use of digitisation, data analysis, AI/ML to differentiate, improve efficiency and strengthen the business.

Business Model Check – As mentioned before, since we operate in CUVVI world, it is extremely important to regularly validate the business model in light of global, economic, regulatory & business specific changes that are ever changing the world order.

Despite these risks, India's large domestic market, stable government, diversified economy, structural reforms, adequate foreign exchange reserves etc. provide significant resilience and cushion against these shocks. However, proactive management of risks will be key to meet the desired expectations and objectives.

11 UAE Regional Interest Group

Written by:
Saurabh Dubey
Managing Director,
Protiviti Member Firm for the
Middle East Region

Saurabh Dubey

Saurabh is currently working as a Managing Director with Protiviti based in Abu Dhabi. He has over 17 years of experience in providing Internal Audit, Risk Advisory, & Consulting services to clients in the GCC and other parts of the Middle East. Saurabh is the Regional Group Chairperson (UAE Chapter) of Institute of Risk Management.

Prior to joining Protiviti, he worked with Ernst & Young.

Written by:
Arjun Manoharan
Commercial Manager,
Premier Insurance Brokers
LLC OPC

Arjun Manoharan

Arjun is currently working as Commercial Manager at Premier Insurance Brokers LLC OPC. He is Chartered Insurance Risk Manager (CII), Technical Specialist with the Institute of Risk Management (IRM) and a Chartered Marketer (CIM) has equipped me with a deep understanding of risk management and marketing and communication principles and practices.

The Future of Risk Management in the United Arab Emirates: Trends and Challenges in 2025

Emerging Risks and Their Drivers

1. Technological Advancements and Cybersecurity Risks

The rapid digital transformation is integral vision of becoming a global hub for technology and innovation. Initiatives such as the Strategy for Artificial Intelligence and Smart Dubai emphasise the importance of interconnected systems and advanced technologies like IoT, AI, and cloud computing.

With increasing digitalisation, the risks related to cybersecurity are the topmost concerns for the organisations. The rise in QR code phishing scams ("quishing") and targeted cyberattacks on critical infrastructure, such as financial institutions and energy sectors, poses significant threats. Investments in AI-driven threat detection and cybersecurity frameworks are pivotal. Many leading organisations are promoting a security-first culture adopting multi-layered defence strategies. Businesses that align with regional cybersecurity initiatives can bolster their resilience against cyber threats.

2. Regulatory Changes and Compliance Risks

The regulatory landscape is evolving, particularly with its focus on data privacy and ESG standards. The commitment to sustainable development is evident in its strategic initiatives like the UAE Net Zero by 2050.

Non-compliance to regulatory requirements can lead to significant penalties, as seen in cases of environmental violations in the construction sector. Organisations can leverage automated compliance monitoring tools. A proactive compliance culture can transform regulatory challenges into competitive advantages.

3. Global Events and Geopolitical Risks

The UAE's strategic position as a global trade hub makes it susceptible to geopolitical risks, such as trade tensions and regional conflicts.

Geopolitical instability can disrupt supply chains, evident during the COVID-19 pandemic when global supply chains faced significant strain. The reliance on international trade means businesses must adapt to fluctuating trade regulations and tariffs. Diversifying supply chains and adopting real-time visibility tools can mitigate disruptions. The investments in infrastructure aim to strengthen supply chain resilience and reduce dependency on specific regions.

4. Economic Shifts and Financial Risks

Economic volatility, driven by global inflation trends and fluctuating oil prices, remains a critical concern. The IMF projects global inflation to decrease, but economic uncertainties persist.

Businesses face liquidity constraints, especially SMEs, due to reduced consumer spending and tighter credit conditions. The economy, although diversified, still experiences vulnerabilities linked to oil price fluctuations. Enhancing financial risk management through predictive analytics and robust liquidity practices can stabilise operations.

6. Employee Retention/ Effective Succession Planning

People-related risk is another key concern for organisations. "The UAE is a growing market and ripe for further investment. Opportunities are good, salaries are high, and achieving a happy work/life balance is not difficult, so attracting talent from all over the world to work in a leading organisation is easy". However, retaining them is a big challenge. There are plenty of opportunities for talented, skilled people to move to better, more senior positions.

There are two immediate knock-on effects from people risks: the first is that companies need to plug skills gaps quickly, especially as they become increasingly reliant on new technologies to drive their business and realise opportunities. Employers are prepared to invest in training for staff to gain professional qualifications, which helps retain skilled people. The other key issue is that succession planning has become increasingly important. Turnover of talented people means that organisations seriously need to consider putting succession plans in place. Risk functions are also not immune to talent retention problems.

"Experienced Risk Managers with key sectoral knowledge and specialist skills are hugely in demand here, so keeping them while you are trying to build a best-in-class risk function can be a very real challenge". A spurt in mergers and acquisitions has also contributed to a "talent exodus". M&A activity is strong in the UAE and the Middle East. From a risk point of view, there needs to be much better employee engagement and a roadmap setting out how people will still be considered important to the organisation. Employers should also make them employees aware of the potential benefits, the possibilities for career progression, and that they might even have additional responsibilities going forward."

5. Supply Chain Risks

Supply chain disruption is probably one of the most important risks. In the UAE, however, sourcing materials is not a problem, "the problem is their timely availability, price, and logistics. Prices have risen and trying to secure goods and services as easily as you did pre-COVID is now much more of a problem for companies.

Logistical issues can mean delays in supply, which affects output, and this is a very real concern for UAE businesses and is therefore a priority for risk functions."

We asked practitioners in the Middle East their thoughts on employment and career development in risk

95% Anticipate that the demand for risk professionals will increase in 2025.

95% Believe new skills will be required in your risk management career

52% believe it is important to pursue additional qualifications once a year to remain competitive

90% identified that it was difficult to hire qualified risk managers in their region.

Challenges and Opportunities for Risk Managers

Keeping Up with Rapid Technological Changes: Risk managers should collaborate with technology experts and invest in digital transformation for learning new innovation/ techniques which can enhance risk management capabilities.

Navigating Complex Regulatory Environments: Building partnerships with legal teams and utilising technology for compliance can simplify processes. There is a strong movement noticed in fintech innovation for ensuring regulatory adherence.

Managing the Human Factor in Cybersecurity: Continuous employee training on cybersecurity is critical. National initiatives like Cyber Pulse Campaign aim to raise awareness and reduce vulnerabilities.

Risk managers in the UAE will transition from traditional roles to becoming strategic advisors, integrating AI and machine learning for deeper risk insights. The emphasis on ESG will redefine risk priorities, fostering innovation and sustainable growth. As the leading organisations continues its journey towards becoming a global economic powerhouse, risk management will play a pivotal role in ensuring resilience and adaptability in a rapidly changing world.

Actionable Recommendations for Risk Practitioners:

1 Enhance Cyber Resilience

- Conduct regular cybersecurity audits and align with National Cybersecurity Strategy.
- Foster a cybersecurity culture with initiatives like "Cyber C3" certification for employees.

2 Strengthen Regulatory Compliance

- Leverage compliance tools and participate in industry forums.
- Adopt centralized compliance management to navigate multi-jurisdictional regulations.

3 Bolster Supply Chain Resilience

- Utilise logistical hubs and real-time supply chain tools to diversify and strengthen supply chains.
- Conduct risk assessments for identifying the possible disruptions and planning of mitigation strategies.

4 Improve Financial Risk Management

- Engage in stress testing supported by the leading financial institution.
- Utilise predictive analytics model/tools to enhance financial forecasting and liquidity management.

12 North America and Caribbean Regional Interest Group

Written by:
Patricia Kidwingira
Chair, IRM North America and Caribbean

Patricia Kidwingira

Patricia Kidwingira, IRMCert, MBA, CCSA, CRMA, LPEC, has 30 years of auditing and program management experience. She has championed ethical practices and unconscious bias initiatives, contributing to key publications for the Ethics & Compliance Initiative.

Patricia has held leadership roles with Toastmasters International, including District Director for District 46 in New York, where she earned the Resilience Award. She is the founding member and current Chair of the Institute of Risk Management North America Regional Group.

1. Cybersecurity Resilience

In today's digital age, cybersecurity threats remain a major risk for organisations. The rapid evolution of cybercrime, geopolitical tensions, and a shortage of skilled professionals have created a challenging environment. Global cybercrime costs are expected to reach $10.5 trillion annually by 2025, with 22,254 CVEs reported in 2024—a 30% increase from the previous year.

These figures highlight the need for robust cybersecurity strategies and proactive measures.

Identified risks include:

- Complex Cyber Attacks: Advanced tools make defense harder.
- Geopolitical Tensions: More state-sponsored attacks.
- Skills Shortage: Not enough cybersecurity professionals.
- Budget Constraints: Limited funds for cybersecurity.
- Targeted Industries: Healthcare, finance, and critical infrastructure are prime targets.
- Remote Work Risks: Home networks and personal devices are vulnerable.

2. The Dual Edge of AI: Opportunities and Risks in 2025

Modern business strategies must balance opportunity created by innovative technologies with their impacts on cybersecurity risk, data governance, and regulations on data privacy. Incorporating AI into business operations is considered vital to efficiency, productivity, and competitiveness, it can also generate digital disruption. The rapid advancements in AI technologies underscore the need for a proactive and adaptive approach to risk management. While AI has the potential to revolutionize industries, it must be developed and deployed responsibly. Ethical AI frameworks are essential to mitigate risks and maximize benefits. The rapid advancement of AI technologies brings significant risks, as highlighted in the World Economic Forum's Global Risks Report and other sources:

- Misinformation and Deep Fakes: AI can create convincing false information.
- Workforce Misuse: Employees might misuse AI tools, leading to errors or unethical outcomes.
- Errors and Misdiagnosis: AI errors can result in incorrect recommendations or diagnoses.
- Intellectual Property Disputes: AI-generated content can lead to ownership conflicts.
- Algorithmic Bias: AI systems can perpetuate biases, influencing decisions unfairly.
- Privacy Concerns: AI can compromise personal data privacy.
- Vulnerability to Cyber-Attacks: AI systems can be targeted by hackers.
- Lack of Transparency: AI decisions can be opaque, reducing trust.

The internal audit foundation noted that or most of the twenty-first century, digital disruption has been a growing and dynamic risk area, and the introduction of user-friendly, zero-cost generative AI tools in 2022 only added to its vexing complexity. It has identified six digital Disruption Risk Drivers:

- Regulations – Compliance now and in the future
- Business opportunity – High risk of missed opportunities
- Financial impact – Fraud/cyber risk and implementation costs
- Politics – Government priorities and guidance
- Public opinion – Market and stakeholder demand
- Social impact – Ethical concerns

Strategies for Mitigation and Adaptation:

- Implement AI Governance Frameworks: Establish guidelines for ethical AI use.
- Enhance Data Security: Protect data integrity and security throughout the AI lifecycle.
- Promote Transparency: Develop explainable AI systems to build trust.

AI technologies will continue to present both opportunities and challenges. Risk managers must adopt ethical frameworks to ensure responsible AI use. The coming years will see increased emphasis on integrating AI into cybersecurity measures and developing robust governance frameworks to address the ethical and societal impacts of AI.

3. Environmental Risk:
A Top Concern for 2025

The World Meteorological organisation (WMO) noted that extreme weather reached dangerous new heights in 2024 with record-breaking temperatures fueled unrelenting heatwaves, drought, wildfire, storms and floods that killed thousands of people and forced millions from their homes.

This exceptional year of extreme weather shows how dangerous life has already become with 1.3°C of human-induced warming and highlights the urgency of moving away from planet-heating fossil fuels as quickly as possible. Extreme weather contributed to the deaths of at least 3,700 people and the displacement of millions in 26 weather events studied in 2024. These were just a small fraction of the 219 events that met WMO trigger criteria, used to identify the most impactful weather events. Environmental risks, remain a top concern for 2025, with rising temperatures, sea level rise, drought, wildfires, and water scarcity threatening ecosystems, economies, and communities, with extreme weather, "risks have become reality".

The internal audit foundation has identified six climate change Risk Drivers:

- Regulations – Sustainability reporting and financing rules
- Financial impact – Cost of extreme weather
- Business opportunity – "Green" business advantage
- Politics – Large differences per country
- Public opinion – Pressure related to sustainability
- Social impact – People and infrastructure impacted by extreme weather

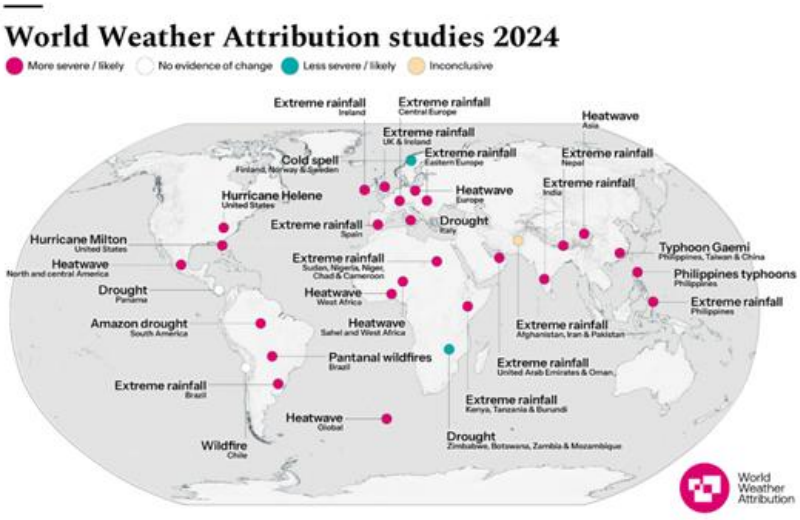
In addition to the various negative impacts:

- Temperature Increase: More frequent heatwaves and intense storms.
- Sea Level Rise: Coastal erosion and increased wildfire activity.
- Biodiversity Loss: Habitat disruption and invasive species.
- Water Scarcity: Reduced crop yields and conflicts over water resources.

There are also opportunities to better manage our planet:

- Early Warning Systems: Advanced systems for heatwaves and floods.
- Infrastructure Resilience: Strengthening infrastructure to withstand extreme weather.
- Water Conservation: Sustainable water-saving strategies.
- Ecosystem Protection: Enhancing biodiversity and natural barriers.
- Climate-Resilient Models: Predictive models to guide policymaking.
- Public Health Systems: Addressing vector-borne diseases.

Understanding the velocity, risk drivers and impact of environmental risks and various opportunities will help prioritise actions. High-velocity, high-impact risks need urgent attention, while slower-developing risks require long-term strategies. Risk managers must stay informed and foster collaboration, emphasising sustainable practices and innovation.



WWA

4. Tackling Geopolitical Uncertainty by Creating Shared Value

The geopolitical uncertainty has significant implications for society, and politics. Prioritising these risks and identifying mitigating factors are essential for effective policy making, and strategic planning. Mitigating factors may include comprehensive immigration reform and enhanced security cooperation.

As noted in the table below, the internal audit foundation noted that geopolitical risks are among the top risks in two regions.

Risk area	Global Average	Africa	Asia Pacific	Europe	Latin America	Middle East	North America
Cybersecurity	73%	64%	64%	83%	74%	66%	88%
Business continuity	51%	57%	62%	32%	49%	63%	41%
Human capital	49%	44%	57%	52%	47%	43%	54%
Digital disruption (including AI)	39%	34%	36%	40%	37%	38%	48%
Regulatory change	38%	32%	32%	46%	45%	27%	47%
Market changes/competition	32%	15%	49%	32%	26%	29%	41%
Financial liquidity	31%	42%	19%	27%	33%	38%	28%
Geopolitical uncertainty	30%	23%	30%	39%	37%	27%	26%
Governance/corporate reporting	25%	31%	22%	20%	18%	41%	16%
Organizational culture	24%	34%	23%	21%	28%	21%	21%
Fraud	24%	42%	22%	14%	32%	27%	9%
Supply chain (including third parties)	23%	16%	24%	29%	17%	26%	29%
Climate change/environment	23%	25%	26%	33%	29%	12%	12%
Communications/reputation	20%	26%	21%	14%	17%	21%	20%
Health/safety	11%	10%	11%	12%	9%	12%	13%
Mergers/acquisitions	6%	4%	4%	8%	4%	8%	8%

If there is a tie for the fifth highest percentage, both percentages are highlighted in a lighter color.

In a geopolitical landscape where countries and international organisations collaborate to address pressing global challenges, value creation transcends local or national concerns and focuses on generating shared global benefits.

Sustainable Development Goals: Many global institutions have outlined universal goals related to sustainability, equity, human rights, and peace. Value creation is increasingly tied to advancing these shared objectives. Businesses and nations are judged not just by their economic output, but by their contribution to solving global issues like poverty, inequality, and climate change.

Risk management, when viewed through the lens of geopolitics and global organisations, involves navigating complex global risks—from climate change and resource depletion to conflict, migration, and pandemics. These risks are interconnected, and their impacts can cascade across borders, affecting both individual countries and the global community.

Incorporating geopolitics and global governance into discussions about innovation, communication, risk management, and value creation allows us to think expansively about our interconnected world. Value creation is no longer just about profits or local success; it is about contributing to the global commons advancing sustainability, social well-being, and human dignity across borders.

13 South Africa Regional Interest Group

George Wandsella IRMCert
Head of Operational Risk
and Fraud at Tyme Bank
ZAF Group Member

Adv. Luxolo Sandlana IRMCert
Advocate of the High Court
of South Africa
ZAF Group Member

Zanele Makhubo IRMCert
Director of Enterprise
Risk Management
ZAF Group Member

Samona Narsee IRMCert
Risk Practitioner
ZAF Group Member

Lea Steenberg IRMCert
Senior Risk Manager, PAREXEL
ZAF Group Member

Dr Riaan Steenberg
NetEd Group

Dr Retha Langa
NetEd Group

Nombulelo Mketi
Siyakhanyisa Consultants

Matema Makgato IRMCert
ZAF Group Member

The South African Landscape

Executive Summary

The South African landscape faces a complex web of interconnected risks and challenges across multiple sectors as it moves towards 2025 and beyond.

Summary of Key Themes:

1. Digital fraud is a rapidly growing threat to South Africa's businesses and government institutions.
2. The legal sector faces challenges related to economic instability, cybersecurity, diversity, and technological adoption.
3. Systemic corruption undermines the rule of law, weakens economic growth, and erodes societal morale.
4. Ethical leadership's role in maintaining the integrity and success of organisations and society.
5. Artificial intelligence presents both opportunities and risks for South Africa's economy and workforce.
6. The education system faces significant challenges, particularly in public education, with private education playing an increasing role.
7. South Africa's healthcare system must overcome the challenges and take the opportunities presented by the global digital transformation of medical health data.
8. Maintaining infrastructure is crucial to mitigating these environmental risks and protecting communities and their livelihoods.
9. The country is undertaking a major transmission lines project to support renewable energy integration.
10. Climate change and extreme weather events pose significant risks, particularly in coastal regions.

To address these multifaceted challenges, South Africa will need to foster innovation, embrace technological advancements responsibly, strengthen public/private partnerships, and prioritise inclusive and sustainable development. By proactively tackling these issues, the country can position itself to harness opportunities for growth while mitigating risks and building resilience across all sectors of society.

Digital Fraud in South Africa: Emerging Trends and Strategic Responses in the Banking Sector

by George Wandsella, Head of Operational Risk and Fraud at Tyme Bank (LLB, BCOM Law, IRMCert, ZAF Regional IRM Committee member)

Digital fraud is rapidly emerging as a critical risk for South African businesses and government, primarily driven by the accelerating adoption of digital banking and increasingly sophisticated cybercriminal tactics. In 2023, banking app fraud represented a staggering 60% of digital banking crimes, marking an alarming 89% increase from the previous year, according to the South African Banking Risk Information Centre (SABRIC). Generative artificial intelligence is emerging as a potent tool for fraudsters, enabling the creation of sophisticated content and exploiting social engineering vulnerabilities such as phishing and vishing. Cybercriminals are strategically leveraging customer trust in social media platforms, a risk further amplified by the persistent threat of data breaches.

The rise of digitally native banks like Tyme Bank—recognized by Forbes as the fastest-growing digital bank in South Africa in 2023—demonstrates a proactive approach. By leveraging cloud computing and artificial intelligence, these institutions are developing robust digital platforms to combat fraud effectively. The economic implications are profound. In 2023, financial losses from digital fraud escalated by 47%, posing a significant threat to economic stability. Businesses are confronting multifaceted challenges, including direct financial losses, increased cybersecurity infrastructure investments, and potential long-term reputational damage.

Practical measures to counter this threat include mandatory multi-factor authentication, consumer awareness campaigns, and investment in AI-driven fraud detection systems. Collaboration between the private sector, government, and international agencies is vital to improve intelligence sharing and enforcement (Deloitte, 2023).

The South African banking sector demonstrates resilience, supported by prudent regulatory oversight. By committing to technological investments and cultivating collaborative relationships among banks and law enforcement agencies, the industry is strategically positioning itself to mitigate digital fraud risks. A critical principle emerging is that cybercrime prevention transcends competitive boundaries—requiring unified, collaborative approaches to effectively combat evolving digital threats.

South Africa's Transmission Lines Mega Project

by Nombulelo Mketi, Siyakhanyisa Consultants (Engineering Services & Project Management)

Electricity in South Africa is transmitted to the rest of the country over thousands of kilometers from power stations which mostly reside near the coalfields in Mpumalanga's Highveld and Limpopo provinces. The newly established National Transmission Company of South Africa (NTCSA) has a great task of building 14 200km of Transmission lines and refurbishment of the existing overhead lines for the evacuation of the Renewable Energy's (RE) generation facilities which mostly lie in the provinces of the Western Cape, Eastern Cape, and Northern Cape. These mega-capital projects aid in the commitment of zero-carbon emissions by 2030 through the energy mix.

During the 2012-2021 Transmission Development Plan (TDP), held in October 2011, Eskom, the country's power utility announced the strategic acquisition of servitude's, an outline of planned investments, including costs, a preview of the impact on customers in terms of prices and service quality, and any additional information as periodically specified by the National Energy Regulator of South Africa (NERSA) including RE projects will ensure implementation by 2020. The power utility has managed to commission 4 300km of Transmission lines in the past 10 years.

In the 2023-2032 TDP which is aligned to the Integrated Resource Plan (IRP), the power utility announced that by 2027 approximately 2890km of extra-high voltage (EHV) Transmission lines and 60 transformers would need to be delivered and the required capital investments are plus 390 Billion ZAR which would need to be raised despite the statutory approvals challenges they are faced with. Capital investments, equipment suppliers and resource capabilities for execution of this project, could hinder the planned target year of 2027 if not effectively addressed.

A dearth in the execution of this target would pose a risk to the RE programme as well as the country's economic development.

The erection of 14,200km of transmission lines would unlock 52GW of new generation capacity, reduce emissions, create job opportunities, bring down energy bills and provide grid stability. The country remains optimistic based on the recent progression in November 2024 by the NTCSA of signing long-term agreements with 28 local companies to construct substations which is part of its TDP that these set targets would be met within the specified timelines.

The Legal Sector in South Africa: An Overview and Emerging Risk Trends

by Luxolo Sandlana, Admitted Attorney of the High Court of South Africa, and current Pupil Advocate (Barrister) at the Pan African Bar Association of South Africa), (LLB(WSU), Higher Cert. in Data Science (EDSA), PGDip in Risk Management (UNISA)

South Africa's legal sector is integral to maintaining justice, governance, and economic stability. Grounded in a hybrid legal system combining Roman-Dutch law and English common law, the sector operates within the framework of the 1996 Constitution, widely regarded as one of the most progressive globally. However, a confluence of challenges, ranging from economic instability to technological disruption, introduced new risks to the profession and industry wide.

This section examines the legal sector in South Africa and explores key emerging risks shaping its evolution.

1. Brief overview of the legal sector in South Africa

South Africa's legal framework supports numerous players, including advocates, attorneys, regulatory bodies, and judiciary members. While the sector has made strides in transformation and innovation, persistent challenges related to accessibility, equity, and efficiency remain. There have been a couple of relatively new promulgated acts and regulations such as the Protection of Personal Information Act (POPIA), which governs the use of personal data in South Africa, impacting the legal profession as firms increasingly adopt digital workflows. Furthermore, the Legal Practice Council (LPC) monitors industry professional standards and transformation goals. These Acts have made a profound impact on the sector and have introduced a host of new risks that previously did not exist before.

2. Emerging Risk Trends in South Africa's Legal Sector

2.1 Economic Instability and Market Pressures

South Africa's sluggish economic growth, estimated at 0.8% in 2023 with high unemployment, has pressured legal firms. Corporate clients are continuously cutting back heavily on legal spending, while smaller firms struggle with liquidity issues. Additionally, limited funding for legal aid affects indigent communities' access to justice.

2.2 Cybersecurity Risks in the Digital Era

South African law firms are increasingly targeted by cybercriminals due to the sensitive client data they handle. Reports indicate that ransomware attacks on the legal sector have surged globally, including in South Africa. There are strict compliance measures for securing personal data, and noncompliance can result in severe penalties, including fines up to ZAR 10 million.

Mitigation Strategies:

- Adopt robust cybersecurity systems, including firewalls, encryption, and multifactor authentication.
- Conduct regular staff training on recognising phishing attacks.

2.3 Transformation and Diversity Challenges

Despite post-apartheid reforms, the legal sector still struggles with racial and gender disparities. According to the LPC, only 29% of attorneys in leadership roles are Black, and women represent just 35% of advocates.

Mitigation Strategy:

- Create mentorship programs for underrepresented groups.
- Enforce employment equity targets and monitor progress transparently.

2.4 Legal Tech Adoption and Technology Risks

The adoption of legal technology (legal tech) is redefining how legal services are delivered. Automation tools for contract analysis, e-discovery, and legal research are streamlining workflows but also posing challenges.

Risks:

- Access to Justice: Technological advancements may widen the digital divide for underserved communities.
- Cost Pressures: Smaller firms struggle to afford cutting-edge solutions, creating disparities.

Mitigation Strategies

- Offer scalable solutions, like cloud-based legal tech, to smaller firms.
- Invest in digital literacy programs for employees and clients alike.

2.5 Climate Change and Environmental Risks

Climate change is an increasingly pressing issue for South Africa, with significant implications for the legal sector. The country is highly vulnerable to climate risks, including extreme weather events, water scarcity, and biodiversity loss. These challenges are compounded by the nation's reliance on coal for energy and its ongoing transition toward renewable energy sources. Legal practitioners are at the forefront of addressing climate change impacts through litigation, compliance advisory, and policy development.

Key Trends:

- Climate-related litigation is on the rise all around the world, including South Africa. These lawsuits frequently involve claims against governments and companies for failing to reduce or adapt to climate risks.

Risks:

- Litigation: Renewable energy projects require extensive compliance with environmental laws, land use regulations, and community engagement processes.
- Carbon Markets: The development of carbon trading mechanisms introduces new regulatory frameworks that legal practitioners must navigate.
- Just Transition: Ensuring fair treatment of workers and communities affected by the move away from coal is another area requiring legal expertise.

Mitigation strategies and opportunities for legal practitioners:

- Advising on Climate Compliance: Firms can specialise in helping clients meet the growing regulatory demands related to emissions reductions, EIAs, and climate risk disclosures.
- Renewable Energy Projects: Legal expertise is crucial in negotiating contracts, securing financing, and obtaining regulatory approvals for renewable energy projects.
- Development of Climate Policy: Lawyers can contribute to shaping national and corporate policies that address climate risks while fostering economic growth.
- Proactive Risk Management: Law firms can position themselves as leaders in climate risk management by offering integrated legal and risk advisory services.

2.6 Regulatory Complexity and Compliance Risks

The dynamic South African regulatory landscape presents significant challenges. Compliance with cross-border data transfer regulations and international sanctions requires constant vigilance.

Moreover, new laws on cryptocurrency and digital assets add layers of complexity. Then there's the ever-present risk of hawala to our financial system.

Mitigation Strategies:

- Technology to track and monitor compliance risks.
- Engage with industry stakeholders to influence regulatory frameworks.

3. Opportunities Amidst Risks

Amidst these challenges, South Africa's legal sector has opportunities for growth. Emerging areas such as cryptocurrency regulation, artificial intelligence law, and renewable energy represent untapped markets. Additionally, technology presents opportunities for increasing efficiency and improving access to justice.

Recommendations:

- Expand into Emerging Fields: Build capacity in niche areas like fintech and environmental law.
- Collaborate with Tech Providers: Partner with legal tech developers to enhance services.
- Pro Bono Initiatives: Strengthen pro bono work to address justice gaps in underserved areas.

Conclusion

South Africa's legal sector is navigating an increasingly complex environment characterised by economic, technological, and societal shifts. By proactively addressing emerging risks, ranging from cybersecurity to regulatory compliance, legal practitioners can sustain relevance and resilience.

Innovation, transformation, and a commitment to ethical practice will ensure the sector continues to uphold justice and advance societal progress.

AI and Risk: A South African Perspective

by Samona Narsee (IRMCert, ZAF Regional IRM Committee member)

South Africa faces significant opportunities and challenges as it embraces artificial intelligence (AI). While AI offers transformative potential, it also brings risks, including workforce displacement, regulatory gaps, and amplified inequality.
With unemployment at 32.9%, sectors like manufacturing and customer service risk job losses, while unequal access to digital infrastructure widens the urban-rural divide.

AI's reliance on data also raises privacy and security concerns under the Protection of Personal Information Act (POPIA) POPIA Guidelines. Meanwhile, businesses face competitive pressures, with AI enabling innovation in sectors like finance, agriculture, and healthcare but threatening those slow to adapt. According to the World Economic Forum Report The Future of Jobs Report 2023 automation could displace millions globally but create new AI-related roles.

Locally, examples like aerobotics in agriculture show how AI can improve productivity. However, without ethical governance, AI risks worsening inequality and bias.

South Africa should focus on Developing robust AI governance frameworks aligned with global standards to address ethical and security concerns, partnering with institutions to upskill workers, especially in vulnerable sectors, and promoting public-private partnerships, such as Tshimologong Digital Innovation Precinct to support inclusive AI innovation and Investing in rural connectivity and support small businesses in adopting AI.

Opportunities include economic growth, improved public services, and entrepreneurial innovation. Looking ahead, South Africa can become a leader in ethical AI development by balancing technological efficiency with human creativity. By adopting proactive strategies, the country can leverage AI's potential for sustainable growth while minimizing its risks.

With unemployment at 32.9%, sectors like manufacturing and customer service risk job losses, while unequal access to digital infrastructure widens the urban-rural divide.

The Future of Healthcare in South Africa: AI, Data, and Innovation

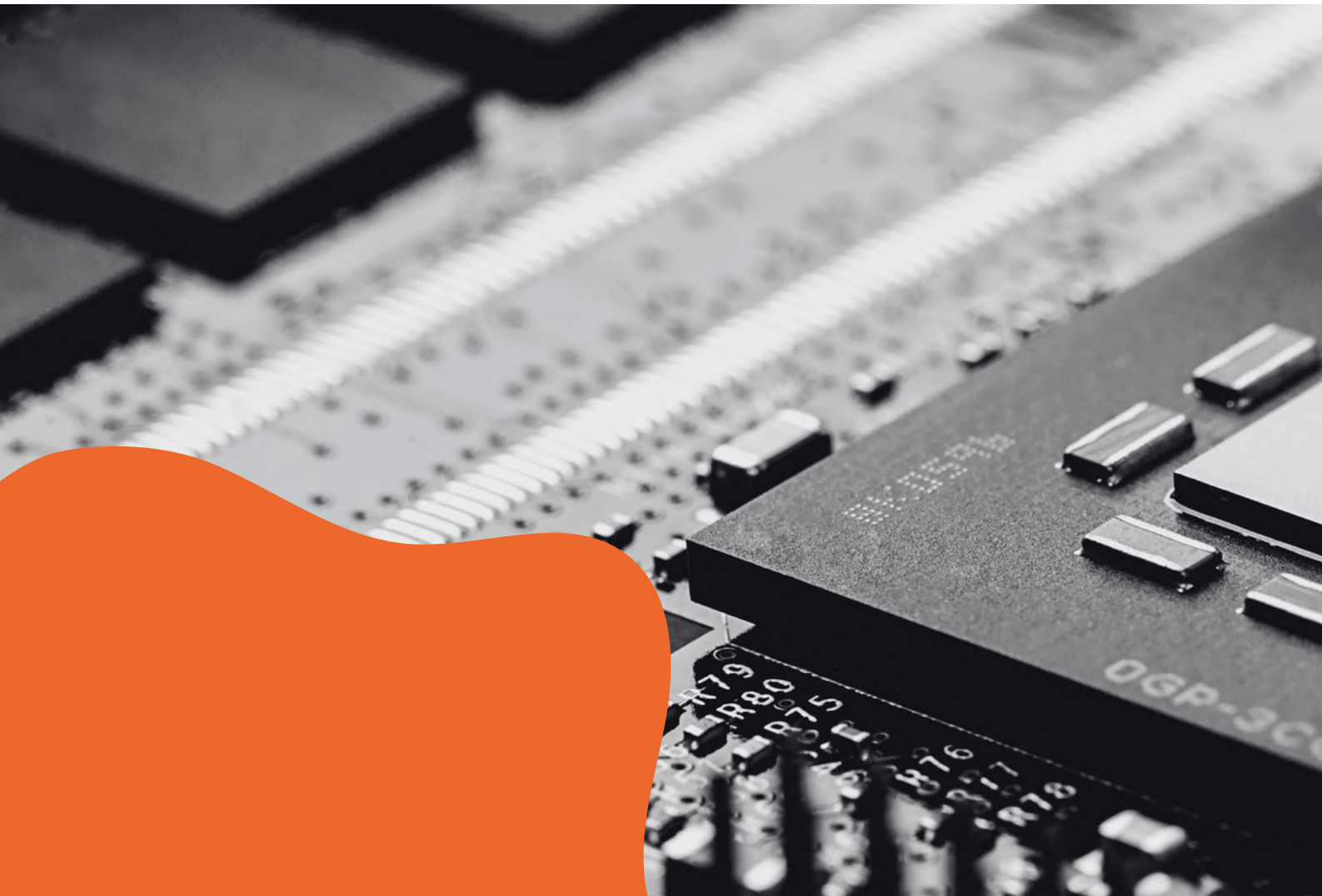
by Lea Steenberg, Senior Risk Manager, PAREXEL

Following the Covid pandemic, and the subsequent geopolitical instability, global regulators have stressed the importance of better healthcare ecosystems to ensure equitable distribution of medical care and access. They emphasise decentralised healthcare, improved data governance, and seamless sharing of medical information to improve public health insights.

It is estimated that 30% of data is health/medical related and that only around 3% of this data is actively analyzed to gain insights to improve public health. With the advent of artificial intelligence, an opportunity has been created to tap into this immense data resource. Artificial Intelligence (AI) has the potential to revolutionise how the pharmaceutical industry and public health sector use medical data. The application of AI promises to reduce the cost and time needed for pharmaceutical research to bring new products to market as well as the opportunity to enhance medical service delivery and reduce human error in medical decision making.

The race to harness real-world data with AI has officially started. If South Africa does not want to be left behind, we must rapidly adopt 'Electronic Health Record' (EHR), and medical record systems within government and private medical institutions that meet international standards such as ICH Good Practice guidelines and Guidelines on computerised systems published by European medicines agency. Improvements in data governance and cyber security facilitate sharable access to high-quality real world data that is fit for purpose. This, in turn, produces reliable, trusted research outputs for both public and private sectors, enhancing our ability to respond to public health threats.

South Africa should seize the opportunity to be a leader in medical industry advancements, technology, and data governance. By collaborating with the pharmaceutical industry, academia, and public health sector, we can implement innovations that will benefit and protect South African citizens.



Systemic Corruption

by Zanele Makhubo, Director of Enterprise Risk Management Gauteng Department of Human Settlement (CFIRM, ZAF Regional IRM Chair)

Systemic corruption undermines the rule of law, weakens economic growth, and erodes societal morale. The state's limited capacity to address systemic corruption allows criminal networks to thrive. Prevention measures against corruption should be societally driven to ensure comprehensive solutions, such as:

- Strengthening Legal Frameworks: Implementing and enforcing robust anti-corruption laws regulations.
- Enhancing Transparency: Promoting transparency in government and business operations to reduce opportunities for corruption.
- Public Awareness Campaigns: Educating the public about the dangers of corruption and encouraging them to report unethical activities.
- Whistleblower Protections: Providing protections for individuals who report corruption to ensure they are not retaliated against.
- Independent Anti-Corruption Agencies: Establishing independent bodies to investigate and prosecute corruption cases.
- Promoting Ethical Leadership: Encouraging ethical behaviour and decision-making in both public and private sectors.
- Community Involvement: Engaging communities in monitoring and reporting corruption to create a collective effort against unethical practices.
- International Cooperation: Collaborating with international organisations to share best practices and support anti-corruption initiatives globally.

Impact of Unethical Leadership

South Africa has been faced with unethical leadership both in the private and public sector which has led to the demised of many companies and public entities. Ethical leadership is crucial for the success of organisations, governments, and countries, while unethical leadership can damage reputation and brand. The following consequences have been observed:

- Damage to Reputation: Unethical leadership has severely harmed organisations and country's reputation and brand.
- Loss of Trust: Stakeholders, including employees, customers, and citizens, have lost trust in the leadership and the institution.
- Decreased Morale: Unethical behavior has led to low morale among employees, citizens, reducing productivity and engagement.
- Financial Losses: Unethical decisions have resulted in financial losses, including decreased revenue, increased costs, and loss of business opportunities.
- Erosion of Ethical Standards: Unethical leadership has created a culture where unethical behavior becomes normalised, further perpetuating misconduct.
- Negative Impact on Society: Unethical leadership has undermined societal values, leading to broader social and economic issues.
- Legal Consequences: No one is held accountable.
- These consequences highlight the importance of ethical leadership in maintaining the integrity and success of organisations and societies.

Environmental Risks

Unmaintained infrastructures, such as drainage systems, contribute to environmental risks in the following ways:

- Increased Flooding: Blocked or poorly maintained drainage systems can lead to water accumulation and severe flooding during heavy rains.
- Property Damage: Floods resulting from unmaintained infrastructure can cause significant damage to homes, businesses, and public properties.
- Loss of Life: Severe floods can result in fatalities, putting communities at risk.
- Health Hazards: Stagnant water from flooding can become a breeding ground for diseases, posing health risks to the affected population.
- Economic Impact: Floods can disrupt local economies, leading to financial losses.
- Environmental Degradation: Flooding can lead to soil erosion, water contamination, and loss of biodiversity.
- Maintaining infrastructure is crucial to mitigating these environmental risks and protecting communities and their livelihoods.

Risk Analysis 2025: Education in South Africa

by Dr Riaan Steenberg and Dr Retha Langa, NetEd Group. The NetEd Group represents leading education brands such as Eduvos, Stellenbosch Business Institute and others in South Africa.

In 2025, the South African public education system faces significant risk due to persistent inequalities between urban and rural areas, compounded by insufficient infrastructure, inadequate digital access, and high dropout rates. The lack of sufficient clarity on a funding model is introducing spontaneous privatisation of education giving rise to private education being a larger portion of education in the South African landscape in 2025 and beyond.

Public Education Risks

Despite substantial government spending, inefficiencies and disparities in resource allocation continue to undermine the quality of public education. Public schools, particularly in rural areas, face challenges such as a lack of qualified teachers, inadequate facilities, and limited access to technology. The COVID-19 pandemic's impact has further widened the digital divide, leaving many rural students without adequate access to remote learning opportunities. These systemic issues contribute to growing socio-economic inequality and limit South Africa's workforce readiness and global competitiveness.

Private Education Risks

While private education plays a critical role in alleviating pressure on the public system and providing specialized, high-quality education, it also faces challenges. The cost of private education creates barriers to accessibility, leading to perceptions of elitism and exclusion while increasingly serving a poorer demographic due to an overburdened public sector. Additionally, regulatory challenges and the need to balance quality with affordability present ongoing risks. The risk of poor funding mechanisms limits the potential impact of private education, however, more parents are choosing this option creating a future education debt scenario.

Overall Education Risks

If these systemic issues are not addressed through increased collaboration between the public and private sectors, the risk of socio-economic stagnation will grow, hampering workforce readiness and limiting South Africa's global competitiveness.

The lack of sufficient clarity on a funding model is introducing spontaneous privatisation of education giving rise to private education being a larger portion of education in the South African landscape in 2025 and beyond.

Climate Change: Impact of acute weather events or extreme weather conditions in South Africa

by Matema Makgato (IRMCert, ZAF Regional IRM Committee member)

Acute weather events are rare at a particular place and season of the year, presenting unusual patterns and severity of impact in terms of location, and timing. The characteristics of acute conditions have proved to intensify in various global regions and vary from country to country in every sense.

The list of Acute weather events from climate change is not exhaustive, and these may include events such as extreme heatwaves, floods, tornadoes, unusual earthquakes. hurricanes, extreme cold waves, drought, tropical cyclone etc. The coastal region of South Africa's province of KwaZulu Natal is counted amongst the many regions adversely hit by climate change events.

As seasons cyclically changes each present increasing occurrence of catastrophic events, devastatingly destroying homes, and state infrastructure from low-veld areas and other areas within the coastal region of KZN. Climate risk is real. The scale of destruction is heartbreaking to the poor and powerless as each event intensify season by season, and yet again the increasing events also continue to proof government's unpreparedness to planning for and responding to the detrimental impact and demands of extreme weather.

Its inability to provide humanitarian relief, restoration of crucial services including provision for shelter and availability of basic infrastructure for household and businesses. This failure to provide adequate response would often result in months of continued hardship experienced by the community and businesses seeking means to recover. Large contributors of climate change are emissions generated by a variety of human activities, including burning fossil fuels, deforestation, improper waste management, energy production, and many other activities.

With coal mining as one of South Africa economy boosters with a yield of 8% of GDP, it too is guilty of contributing towards this global crisis. Extreme weather events have increase to the point that World Meteorological day 2022 theme was Early warning and Early action, focused on climate change. There is a significant need of climate change awareness for decision makers within the state.

4/10 practitioners in Africa identified climate and sustainability risk integration as a priority focus for African organisations in 2025

To understand the crucial need of being prepared for the unknown environmental events, to ensure they're able to foster and adopt practices to manage extreme weather conditions, for the coastal region of KZN to make necessary support ready, ensure prepared , avail adequate resources to reduce the catastrophic risk and impact on communities from climate event.

Conclusion

South Africa faces a complex web of interconnected challenges and opportunities as it approaches 2025 and beyond. The country must improve equitable opportunities, particularly in education and digital access, while also adapting to rapid technological change and the impacts of climate change. Cybersecurity and digital fraud pose growing threats to the economy and government institutions.

However, South Africa also has opportunities to leverage its strengths in areas such as renewable energy, private education, and healthcare innovation. The country's ability to ethically navigate these challenges while capitalising on opportunities will be crucial in determining its future economic competitiveness and social progress. Collaboration between public and private sectors, investment in digital infrastructure and skills development, and proactive approaches to infrastructure maintenance and climate resilience will be key factors in shaping South Africa's trajectory in the coming years. By proactively addressing these risks, the country can position itself to harness opportunities for growth while building resilience in an increasingly complex global landscape.

Risk in Africa

With 4 Regional Groups, and a dedicated office, the IRM aims to drive the development of the risk management profession and champion best practices throughout Africa.

Data Analysis:

Top Emerging Risk in Africa

86% of practitioners polled highlighted Cybersecurity as the top emerging risk

ISO 31000 was the top risk management standard in Africa

The integration of risk management standards was identified as one of the biggest challenges in African organisations

64% of risk professionals identified AI and ML as biggest impacts to risk management practices in 2025.

70% of risk professionals believe that risk management is not given the most importance in decision making processes.

72% of risk professionals believe that their organisations are averagely prepared for managing climate related risks in the next 5 years identifying a significant area for improvement.

40% of risk professionals believe Climate and sustainability risk integration will be a priority focus in 2025.

We asked which aspect of risk management has required the most significant investment or change in Africa this past year to understand better how risk has evolved in 2024?

66% identified Technology and digital risk management

33% identified Cybersecurity and Geopolitical stability as the top emerging risks in 2025

Acknowledgements

We extend our sincere gratitude to all those who contributed to this year's Risk Trends report. As the Institute of Risk Management continues to expand internationally, we are committed to our collaboration with risk professionals worldwide to enhance our understanding of the global risk landscape.

We also want to thank all the practitioners who participated in the Risk Trends Survey. Your valuable insights have played a crucial role in shaping a comprehensive perspective on risk across a multitude of industries and roles.

Project lead and layout:
Andrew Demetriou, Content Manager

Data analysis:
Danial Ibrahim, Marketing Manager

Proofing:
Ly Na Ho, Junior Marketing Executive
Nick Webber, Digital Marketing Coordinator

Want to get in touch?

Contact one of our team members and we'll help you with whatever you need:

Enquiries - enquiries@theirm.org

Student Services - studentservices@theirm.org

Membership - membership@theirm.org

Marketing - marketing@theirm.org

Training - training@theirm.org

Finance - finance@theirm.org

Events - events@theirm.org

As we look to the future, ERM's role as a strategic enabler becomes ever more vital. It empowers businesses to navigate uncertainty with confidence, adapt to rapid change, and build long-term value.

- Stephen Sidebottom, IRM Chair